EIOPA-BoS-20-002

Leitlinien zum Outsourcing an Cloud-Anbieter

Inhalt

Einleitung

1. Gemäß Artikel 16 der Verordnung (EU) Nr. 1094/2010[1] gibt die EIOPA Leitlinien heraus, die Versicherungs- und Rückversicherungsunternehmen als Orientierung bei der Anwendung der in der Richtlinie 2009/138/EG[2] („Solvabilität II") und der Delegierten Verordnung (EU) Nr. 2015/35[3] der Kommission („Delegierte Verordnung") festgelegten Regelungen für das Outsourcing an Anbieter von Cloud-Diensten dienen sollen.

2. Die vorliegenden Leitlinien stützen sich auf Artikel 13 Absatz 28, Artikel 38 und Artikel 49 der Richtlinie „Solvabilität II" und auf Artikel 274 der Delegierten Verordnung. Zudem knüpfen sie an die Orientierungshilfen an, die die EIOPA mit den Leitlinien zum Governance-System (EIOPA-BoS-14/253) ausgearbeitet hat.

3. Die vorliegenden Leitlinien richten sich an Behörden, die dafür zuständig sind, Versicherungs- und Rückversicherungsunternehmen (zusammen „Unternehmen" genannt) Hilfestellung bei der Einhaltung der Anforderungen zu geben, die in den vorgenannten Rechtsakten für das Outsourcing an Cloud-Anbieter festgelegt sind.

4. Die Leitlinien finden sowohl auf einzelne Unternehmen als auch sinngemäß auf Gruppen Anwendung.[4]

   Die Einrichtungen, die anderen sektorbezogenen Anforderungen unterliegen und Teil einer Gruppe sind, sind als einzelnes Unternehmen vom Anwendungsbereich dieser Leitlinien ausgenommen, da sie verpflichtet sind, die sektorbezogenen besonderen Anforderungen und die entsprechenden von der Europäischen Wertpapier- und Marktaufsichtsbehörde und der Europäischen Bankenaufsichtsbehörde bereitgestellten Leitlinien anzuwenden.

5. Im Falle einer Auslagerung innerhalb der Gruppe und einer Weiterauslagerung an Cloud-Anbieter sollten diese Leitlinien in Verbindung mit den Regelungen der von der EIOPA erstellten Leitlinien zum Governance-System für Auslagerungen innerhalb der Gruppe angewandt werden.

6. Bei der Einhaltung dieser Leitlinien bzw. bei der Überwachung der Einhaltung dieser Leitlinien sollten Unternehmen und zuständige Behörden den Grundsatz der Verhältnismäßigkeit[5] wahren und die Kritikalität oder Bedeutung der an Cloud-Anbieter ausgelagerten Dienstleistung berücksichtigen. Nach dem Grundsatz der Verhältnismäßigkeit sollte sichergestellt sein, dass Governance-Vereinbarungen unter anderem Vereinbarungen über Outsourcing an Cloud-Anbieter in einem angemessenen Verhältnis zu der Art, dem Umfang und der Komplexität der zugrunde liegenden Risiken stehen.

7. Die vorliegenden Leitlinien sollten in Verbindung mit den von der EIOPA erstellten Leitlinien zum Governance-System und den in Absatz 1 aufgeführten aufsichtsrechtlichen Verpflichtungen und unbeschadet dieser Leitlinien und Verpflichtungen gelesen werden.

---

[1] Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331, 15.12.2010, S. 48).

[2] Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

[3] Delegierte Verordnung (EU) 2015/35 der Kommission vom 10. Oktober 2014 zur Ergänzung der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 12 vom 17.1.2015, S. 1).

[4] Artikel 212 Absatz 1 der Richtlinie „Solvabilität II".

[5] Artikel 29 Absatz 3 der Richtlinie „Solvabilität II".

Begriffsbestimmungen

8. Für Begriffe, die in diesen Leitlinien nicht definiert werden, gelten die Begriffsbestimmungen der in der Einleitung genannten Rechtsakte.

9. Für die Zwecke der vorliegenden Leitlinien bezeichnet darüber hinaus der Begriff

Dienstleister	einen Dritten, der auf der Grundlage einer Auslagerungsvereinbarung ein Verfahren, eine Dienstleistung oder eine Tätigkeit bzw. Teile eines Verfahrens, einer Dienstleistung oder einer Tätigkeit ausführt;
Cloud-Anbieter	einen Dienstleister im Sinne der vorstehenden Begriffsbestimmung, der für die Erbringung von Cloud-Diensten auf der Grundlage einer Auslagerungsvereinbarung zuständig ist;
Cloud-Dienste	Dienste, die mithilfe von Cloud-Computing erbracht werden, also einem 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 minimalem Verwaltungsaufwand oder minimaler Interaktion des Dienstleisters bereitstellen lässt;
Öffentliche Cloud	Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann;
Private Cloud	Cloud-Infrastruktur, die ausschließlich von einem einzelnen Unternehmen genutzt werden kann;
Community-Cloud	Cloud-Infrastruktur, die ausschließlich von einer bestimmten Gemeinschaft von Unternehmen, d. h. von mehreren Unternehmen einer einzelnen Gruppe, genutzt werden kann;
Hybrid-Cloud	Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.

Beginn der Anwendung

10. Diese Leitlinien finden ab dem 1. Januar 2021 bei allen Vereinbarungen über Cloud-Outsourcing Anwendung, die an oder nach diesem Zeitpunkt geschlossen bzw. geändert werden.

11. Die Unternehmen sollten bestehende Vereinbarungen über Cloud-Outsourcing, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, überprüfen und entsprechend ändern, um sicherzustellen, dass die vorliegenden Leitlinien spätestens am 31. Dezember 2022 eingehalten werden.

12. Falls die Überprüfung von Vereinbarungen über Cloud-Outsourcing, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, am 31. Dezember 2022 nicht abgeschlossen ist, sollte das Unternehmen seine Aufsichtsbehörde[6] entsprechend benachrichtigen und dabei auch angeben, welche Maßnahmen zur Fertigstellung der Überprüfung bzw. welche potenzielle Ausstiegsstrategie es geplant

[6] Artikel 13 Absatz 10 der Richtlinie „Solvabilität II".

hat. Die Aufsichtsbehörde kann mit dem Unternehmen gegebenenfalls eine Verlängerung der Frist für den Abschluss der Überprüfung vereinbaren.

13. Die Aktualisierung der Strategien und internen Verfahren des Unternehmens sollte (soweit erforderlich) spätestens am 1. Januar 2021 abgeschlossen sein, wohingegen die Dokumentationsanforderungen für Vereinbarungen über Cloud-Outsourcing, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, spätestens am 31. Dezember 2022 umgesetzt sein sollten.

Leitlinie 1 – Cloud-Dienste und Outsourcing

14. Das Unternehmen sollte prüfen, ob eine Vereinbarung mit einem Cloud-Anbieter unter die Bestimmung des Begriffs „Outsourcing" nach der Richtlinie „Solvabilität II" fällt. Bei dieser Prüfung sollte Folgendes berücksichtigt werden:

a. Wird die ausgelagerte operative Funktion bzw. Tätigkeit (oder Teile der Funktion bzw. der Tätigkeit) in periodischen Abständen oder kontinuierlich ausgeführt?

b. Würde diese operative Funktion oder Tätigkeit (oder Teile der Funktion bzw. der Tätigkeit) in der Regel zu den operativen Funktionen oder Tätigkeiten zählen, die das Unternehmen im Rahmen seiner laufenden Geschäftstätigkeit ausführen würde oder könnte, auch dann, wenn das Unternehmen diese operative Funktion oder Tätigkeit in der Vergangenheit nicht ausgeführt hat?

15. Wenn sich eine Vereinbarung mit einem Cloud-Anbieter auf mehrere operative Funktionen oder Tätigkeiten erstreckt, sollte das Unternehmen alle Aspekte der Vereinbarung bei seiner Prüfung berücksichtigen.

16. Wenn das Unternehmen operative Funktionen oder Tätigkeiten an andere Dienstleister als Cloud-Anbieter auslagert, die aber bei der Erbringung ihrer Dienstleistungen in hohem Maße auf Cloud-Infrastrukturen angewiesen sind, (wenn z. B. der Cloud-Anbieter Teil einer Weiterauslagerungskette ist) fällt die Vereinbarung über ein solches Outsourcing in den Anwendungsbereich dieser Leitlinien.

Leitlinie 2 – Allgemeine Governance-Grundsätze für Cloud-Outsourcing

17. Unbeschadet von Artikel 274 Absatz 3 der Delegierten Verordnung sollte das Verwaltungs-, Management- oder Aufsichtsorgan des Unternehmens sicherstellen, dass Entscheidungen über die Auslagerung von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an Cloud-Anbieter auf der Grundlage einer eingehenden Risikobewertung getroffen werden, bei der auch alle relevanten Risiken berücksichtigt werden, die sich aus der Vereinbarung z. B. für die Informations- und Kommunikationstechnologie (IKT), die Geschäftskontinuität, die Einhaltung der Rechtsvorschriften und den Aspekt der Konzentration ergeben, sowie sonstige betriebliche Risiken und ggf. Risiken im Zusammenhang mit der Datenmigration und/oder der Durchführungsphase.

18. Bei Auslagerungen von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an Cloud-Anbieter sollte das Unternehmen gegebenenfalls überlegen, welche Änderungen sich aus den Vereinbarungen über Cloud-Outsourcing für sein eigenes Risikoprofil bei der unternehmenseigenen Risiko- und Solvabilitätsbeurteilung ergeben.

19. Die Nutzung von Cloud-Diensten sollte in Einklang mit den Strategien des Unternehmens (z. B. der IKT-Strategie, der Informationssicherheitsstrategie, der

betrieblichen Risikomanagementstrategie) und mit den internen Strategien und Verfahren stehen, die erforderlichenfalls aktualisiert werden sollten.

Leitlinie 3 – Aktualisierung der schriftlich festgelegten Auslagerungsstrategie

20. Bei Auslagerungen an Cloud-Anbieter sollte das Unternehmen die schriftlich festgelegte Auslagerungsstrategie (z. B. durch die Überprüfung der Strategie, die Aufnahme eines gesonderten Anhangs oder die Ausarbeitung von neuen speziellen Strategien) und die sonstigen relevanten internen Strategien (z. B. für Informationssicherheit) aktualisieren und dabei die Besonderheiten des Cloud-Outsourcing zumindest in Bezug auf folgende Aspekte berücksichtigen:

a. Aufgaben und Zuständigkeiten der betroffenen Unternehmensfunktionen insbesondere des Verwaltungs-, Management- oder Aufsichtsorgans, und der für IKT, Informationssicherheit, Einhaltung von Vorschriften, Risikomanagement und interne Prüfungen zuständigen Funktionen;

b. Prozesse und Berichtsverfahren, die für die Genehmigung, Durchführung, Überwachung, Verwaltung und ggf. Verlängerung von Vereinbarungen über Cloud-Outsourcing, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, erforderlich sind;

c. Kontrolle von Cloud-Diensten in einem angemessenen Verhältnis zu der Art, dem Umfang und der Komplexität der Risiken, die mit den erbrachten Dienstleistungen einhergehen; sie beinhaltet unter anderem 1. die Risikobewertung von Vereinbarungen über Cloud-Outsourcing und Due-Diligence-Prüfung vonCloud-Anbietern, unter anderem in Bezug auf die Häufigkeit der Risikobewertung; 2. die Überwachung und Verwaltungskontrollen (z. B. Überprüfung der Dienstgütevereinbarung); 3. die Sicherheitsstandards und Sicherheitskontrollen;

d. Hinweis auf die in der Leitlinie 10 aufgeführten vertraglich festgelegten Anforderungen hinsichtlich des Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten;

e. Dokumentationsanforderungen und schriftliche Mitteilung an die Aufsichtsbehörde in Bezug auf das Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten;

f. Verpflichtung in Bezug auf die einzelnen Vereinbarungen über Cloud-Outsourcing, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, zur Erarbeitung einer dokumentierten und ggf. hinreichend erprobten „Ausstiegsstrategie", die in einem angemessenen Verhältnis zu der Art, dem Umfang und der Komplexität der mit den erbrachten Dienstleistungen einhergehenden Risiken stehen. Die Ausstiegsstrategie kann mehrere Beendigungsverfahren umfassen, die die Beendigung, Wiedereingliederung oder Übertragung der Dienstleistungen, die Gegenstand der Vereinbarung über Cloud-Outsourcing sind, einschließen, aber nicht unbedingt auf diese Maßnahmen beschränkt sind.

Leitlinie 4 – Schriftliche Mitteilung an die Aufsichtsbehörde

21. Die Anforderungen zur schriftlichen Mitteilung, die in Artikel 49 Absatz 3 der Richtlinie „Solvabilität II" festgelegt sind und in den von der EIOPA erstellten Leitlinien zum Governance-System näher ausgeführt werden, gelten für alle Auslagerungen von kritischen oder wichtigen operativen Funktionen und Tätigkeiten anCloud-Anbieter. Falls eine ausgelagerte operative Funktion oder Tätigkeit, die

zunächst als nicht kritisch oder nicht wichtig eingestuft war, kritisch oder wichtig wird, sollte das Unternehmen die Aufsichtsbehörde entsprechend informieren.

22. Die schriftliche Mitteilung des Unternehmens sollte unter Wahrung des Grundsatzes der Verhältnismäßigkeit zumindest die folgenden Angaben enthalten:

a. eine knapp gefasste Beschreibung der ausgelagerten operativen Funktion oder Tätigkeit;

b. das Datum des Beginns und ggf. das Datum der nächsten Vertragsverlängerung, das Datum des Endes und/oder die Kündigungsfristen für den Cloud-Anbieter und das Unternehmen;

c. das für die Vereinbarung über Cloud-Outsourcing geltende Recht;

d. den Namen desCloud-Anbieters, die Handelsregisternummer des Unternehmens, (ggf.) die Rechtsträgerkennung, die eingetragene Adresse und sonstige relevante Kontaktangaben sowie (ggf.) den Namen des Mutterunternehmens; bei Gruppen ist anzugeben, ob der Cloud-Anbieter Teil der Gruppe ist oder nicht;

e. Cloud-Dienste und Bereitstellungsmodelle (d. h. öffentliche oder private Cloud oder Hybrid- oder Community-Cloud) und die spezifische Art der betreffenden Daten sowie die Standorte (d. h. Länder oder Regionen), an denen diese Daten gespeichert werden;

f. eine Kurzzusammenfassung der Gründe, weshalb die ausgelagerte operative Funktion oder Tätigkeit als kritisch oder wichtig gilt;

g. das Datum der zuletzt durchgeführten Bewertung der Kritikalität oder Bedeutung der ausgelagerten operativen Funktion oder Tätigkeit.

Leitlinie 5 – Dokumentationsanforderungen

23. Das Unternehmen sollte im Rahmen seines Governance- und Risikomanagementsystems Aufzeichnungen über seine Vereinbarungen über Cloud-Outsourcing z. B. in Form eines speziellen, laufend aktualisierten Registers führen. Das Unternehmen sollte für die Dauer einer angemessenen, nationalen Rechtsvorschriften unterliegenden Aufbewahrungsfrist zudem Aufzeichnungen über beendete Vereinbarungen über Cloud-Outsourcing führen.

24. Bei Auslagerungen von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten sollte das Unternehmen alle im Folgenden aufgeführten Angaben erfassen:

a. die Angaben, die der Aufsichtsbehörde gemäß Leitlinie 4 mitzuteilen sind;

b. bei Gruppen: die Versicherungs- und Rückversicherungsunternehmen und sonstigen Unternehmen, die zu Aufsichtszwecken konsolidiert wurden und die Cloud-Dienste nutzen;

c. das Datum der zuletzt durchgeführten Risikobewertung und eine kurze Zusammenfassung der wichtigsten Ergebnisse;

d. die Person bzw. das Entscheidungsgremium (z. B. das Verwaltungs-, Management- oder Aufsichtsorgan) im Unternehmen, die bzw. das die Vereinbarung über Cloud-Outsourcing genehmigt hat;

e. gegebenenfalls das Datum der zuletzt durchgeführten sowie das der nächsten geplanten Prüfung;

f. die Namen etwaiger Unterauftragnehmer, an die wesentliche Teile einer kritischen oder wichtigen operativen Funktion oder Tätigkeit weiterausgelagert

werden, einschließlich der Länder, in denen die Unterauftragnehmer registriert sind, in denen die Dienstleistung erbracht wird, und gegebenenfalls der Orte (d. h. Länder oder Regionen), in denen die Daten gespeichert werden;

g. ein Ergebnis der Bewertung der Ersetzbarkeit des Cloud-Anbieters (problemlos, schwierig oder unmöglich);

h. die Angabe, ob die ausgelagerte kritische oder wichtige operative Funktion oder Tätigkeit termingebundene Geschäftsvorgänge unterstützt;

i. die veranschlagten jährlichen Haushaltskosten;

j. die Angabe, ob das Unternehmen für den Fall der Kündigung einer Vertragspartei oder der Unterbrechung der Dienstleistungserbringung durch den Cloud-Anbieter über eine Ausstiegsstrategie verfügt.

25. Bei Auslagerungen von nicht kritischen oder nicht wichtigen operativen Funktionen oder Tätigkeiten sollte das Unternehmen auf der Grundlage der Art, des Umfangs und der Komplexität der Risiken, die mit den vom Cloud-Anbieter erbrachten Dienstleistungen verbunden sind, festlegen, welche Informationen aufzuzeichnen sind.

26. Das Unternehmen sollte der Aufsichtsbehörde auf Ersuchen alle Informationen zur Verfügung stellen, die diese Behörde benötigt, um die Aufsicht über das Unternehmen führen zu können; dies beinhaltet eine Ausfertigung der Auslagerungsvereinbarung.

Leitlinie 6 – Analyse vor der Auslagerung

27. Vor dem Abschluss einer Vereinbarung mit Cloud-Anbietern sollte das Unternehmen:

a. in Einklang mit der Leitlinie 7 prüfen, ob die Vereinbarung über Cloud-Outsourcing eine kritische oder wichtige operative Funktion oder Tätigkeit betrifft;

b. in Einklang mit der Leitlinie 8 alle relevanten Risiken der Vereinbarung über Cloud-Outsourcing ermitteln und bewerten;

c. in Einklang mit der Leitlinie 9 eine angemessene Due-Diligence-Prüfung des potenziellen Cloud-Anbieters vornehmen;

d. in Einklang mit den Anforderungen nach Artikel 274 Absatz 3 Buchstabe b der Delegierten Verordnung Interessenkonflikte, die sich aus der Auslagerung ergeben können, ermitteln und bewerten.

Leitlinie 7 – Prüfung kritischer oder wichtiger operativer Funktionen und Tätigkeiten

28. Vor dem Abschluss einer Auslagerungsvereinbarung mit Cloud-Anbietern sollte das Unternehmen prüfen, ob die Vereinbarung über Cloud-Outsourcing eine operative Funktion oder Tätigkeit betrifft, die kritisch oder wichtig ist. Bei dieser Prüfung sollte das Unternehmen ggf. in Erwägung ziehen, ob die Vereinbarung in Zukunft potenziell kritisch oder wichtig werden könnte. Ferner sollte das Unternehmen die Kritikalität oder Bedeutung der operativen Funktion oder Tätigkeit, die bereits an Cloud-Anbieter ausgelagert wurden, einer neuerlichen Prüfung unterziehen, wenn sich erhebliche Änderungen der Art, des Umfangs oder der Komplexität der mit der Vereinbarung verbundenen Risiken ergeben.

29. Bei der Prüfung sollte das Unternehmen zusammen mit dem Ergebnis der Risikobewertung zumindest die nachstehend aufgeführten Faktoren berücksichtigen:

a. die potenziellen Auswirkungen etwaiger erheblicher Störungen der ausgelagerten operativen Funktion oder Tätigkeit bzw. der Nichterbringung der Dienstleistungen durch den Cloud-Anbieter in der vereinbarten Dienstleistungsgüte, auf Folgendes:

   i. die kontinuierliche Einhaltung seiner aufsichtsrechtlichen Verpflichtungen;

   ii. die kurz- und die langzeitige Widerstandsfähigkeit und Tragfähigkeit der Finanzen und der Solvabilität;

   iii. die Geschäftskontinuität und die operative Widerstandsfähigkeit;

   iv. das operative Risiko, einschließlich der mit dem Verhalten und dem Bereich IKT verbundenen Risiken und der rechtlichen Risiken;

   v. die Reputationsrisiken;

b. die potenziellen Auswirkungen der Vereinbarung über Cloud-Outsourcing auf die Fähigkeit des Unternehmens,

   i. alle relevanten Risiken zu ermitteln, zu überwachen und zu steuern;

   ii. sämtliche gesetzlichen und regulatorischen Anforderungen zu erfüllen;

   iii. angemessene Prüfungen in Bezug auf die ausgelagerte operative Funktion oder Tätigkeit durchzuführen;

c. die aggregierte Exposition des Unternehmens (ggf. und/oder der Gruppe) gegenüber einem einzigen Cloud-Anbieter und die potenziellen kumulativen Auswirkungen von Auslagerungsvereinbarungen in einem einzigen Geschäftsbereich;

d. Umfang und Komplexität aller Geschäftsbereiche des Unternehmens, die von der Vereinbarung über Cloud-Outsourcing betroffen sind;

e. die Fähigkeit, die vorgeschlagene Vereinbarung über Cloud-Outsourcing, falls erforderlich oder wünschenswert, einem anderen Cloud-Anbieter zu übertragen bzw. die Dienstleistungen wieder im eigenen Unternehmen zu erbringen (Ersetzbarkeit);

f. den Schutz personenbezogener und nicht personenbezogener Daten und die potenziellen Auswirkungen einer Verletzung der Geheimhaltung oder eines Versäumnisses, Datenverfügbarkeit und Datenintegrität unter anderem nach Maßgabe der Verordnung (EU) 2016/679[7] sicherzustellen, auf das Unternehmen, auf Versicherungsnehmer und andere relevante Beteiligte. Das Unternehmen sollte insbesondere Daten berücksichtigen, die als Betriebsgeheimnis und/oder als sensible Daten gelten (z. B. Gesundheitsdaten von Versicherungsnehmern).

Leitlinie 8 – Bewertung der mit dem Cloud-Outsourcing verbundenen Risiken

30. Generell gilt, dass das Unternehmen einen Ansatz wählen sollte, der in einem angemessenen Verhältnis zu der Art, dem Umfang und der Komplexität der Risiken steht, die mit den an Cloud-Anbieter ausgelagerten Dienstleistungen einhergehen. Dies bedeutet unter anderem, dass das Unternehmen die potenziellen Auswirkungen

[7] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

eines etwaigen Cloud-Outsourcing insbesondere im Hinblick auf seine operativen Risiken und seine Reputationsrisiken prüfen sollte.

31. Bei Auslagerungen von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an Cloud-Anbieter sollte das Unternehmen:

a. die zu erwartenden Vorteile und Kosten berücksichtigen, die mit der vorgeschlagenen Vereinbarung über Cloud-Outsourcing verbunden sind; dies beinhaltet auch die Abwägung etwaiger erheblicher Risiken, die verringert werden oder besser gesteuert werden können, gegen etwaige erhebliche Risiken, die sich aus der vorgeschlagenen Vereinbarung über Cloud-Outsourcing ergeben können;

b. sofern anwendbar und angemessen prüfen, welche Risiken, einschließlich der rechtlichen Risiken, der Risiken im IKT-Bereich, der Risiken für die Einhaltung von Vorschriften sowie der Reputationsrisiken, und welche aufsichtsrechtlichen Einschränkungen sich aus folgenden Faktoren ergeben:

   i. aus dem ausgewählten Cloud-Dienst und den vorgeschlagenen Bereitstellungsmodellen (d. h. öffentliche oder private Cloud oder Hybrid- oder Community-Cloud);

   ii. aus der Migration und/oder der Ausführung;

   iii. aus den Tätigkeiten und den zugehörigen Daten und Systemen, die für eine Auslagerung in Betracht gezogen werden (bzw. die ausgelagert wurden), und ihrer Sensitivität und den erforderlichen Sicherheitsmaßnahmen;

   iv. aus der politischen Stabilität und der Sicherheitslage der Länder (innerhalb oder außerhalb der EU), in denen die ausgelagerten Dienstleistungen bereitgestellt werden bzw. bereitgestellt werden können und in denen die Daten gespeichert werden bzw. vermutlich gespeichert werden. Bei der Prüfung sollte Folgendes berücksichtigt werden:

      1. die geltenden Gesetze, einschließlich der Rechtsvorschriften zum Datenschutz;

      2. die geltenden Bestimmungen zur Rechtsdurchsetzung;

      3. die insolvenzrechtlichen Vorschriften, die beim Ausfall eines Dienstleisters Anwendung fänden, und etwaige Einschränkungen, die sich aus der dringenden Wiederherstellung der Daten des Unternehmens ergeben könnten;

   v. die Weiterauslagerung einschließlich der zusätzlichen Risiken, die entstehen können, falls der Unterauftragnehmer in einem Drittland oder in einem anderen Land als der Cloud-Anbieter angesiedelt ist, und das Risiko, dass langwierige und komplizierte Weiterauslagerungsketten das Unternehmen in seiner Fähigkeit, seine kritischen oder wichtigen operativen Funktionen oder Tätigkeiten zu überwachen, und Aufsichtsbehörden in ihrer Fähigkeit, eine wirksame Aufsicht über diese Unternehmen zu leisten, beeinträchtigen könnten;

   vi. das Konzentrationsrisiko der Unternehmen insgesamt gegenüber einem einzigenCloud-Anbieter, wobei auch die Auslagerung an einenCloud-Anbieter, der nicht problemlos ersetzbar ist, oder mehrere Auslagerungsvereinbarungen mit einem einzigen Cloud-

Anbieter einbezogen werden sollten. Bei der Prüfung des Konzentrationsrisikos sollte das Unternehmen (ggf. und/oder die Gruppe) alle Vereinbarungen über Cloud-Outsourcing zugrunde legen, die es mit diesem Cloud-Anbieter geschlossen hat.

32. Die Risikobewertung sollte vor einem Cloud-Outsourcing durchgeführt werden. Falls das Unternehmen Kenntnis von erheblichen Mängeln und/oder erheblichen Veränderungen bei den erbrachten Dienstleistungen oder der Situation des Cloud-Anbieters erlangt, sollte die Risikobewertung umgehend überprüft oder erneut durchgeführt werden. Bei einer Erneuerung einer Vereinbarung über Cloud-Outsourcing, die den Inhalt und den Umfang dieser Vereinbarung betrifft, (z. B. Erweiterung des Umfangs oder Aufnahme von kritischen oder wichtigen operativen Funktionen, die zuvor nicht inbegriffen waren, in den Vereinbarungsumfang) sollte erneut eine Risikobewertung durchgeführt werden.

Leitlinie 9 – Due-Diligence-Prüfung des Cloud-Anbieters

33. Das Unternehmen sollte durch sein Auswahl- und Bewertungsverfahren sicherstellen, dass der Cloud-Anbieter den Kriterien seiner schriftlich festgelegten Auslagerungsstrategie entspricht.

34. Die Due-Diligence-Prüfung des Cloud-Anbieters sollte vor einer Auslagerung von operativen Funktionen oder Tätigkeiten erfolgen. Wenn das Unternehmen eine zweite Vereinbarung mit einem Cloud-Anbieter schließt, der bereits einer Prüfung unterzogen wurde, sollte es auf der Grundlage eines risikobasierten Ansatzes feststellen, ob eine zweite Due-Diligence-Prüfung erforderlich ist. Falls das Unternehmen Kenntnis von erheblichen Mängeln und/oder erheblichen Veränderungen in Bezug auf die erbrachten Dienstleistungen oder die Situation des Cloud-Anbieters erlangt, sollte die Due-Diligence-Prüfung umgehend überprüft oder erneut durchgeführt werden.

35. Wenn kritische oder wichtige operative Funktionen für ein Cloud-Outsourcing vorgesehen sind, sollte die Due-Diligence-Prüfung eine Bewertung der Eignung des Cloud-Anbieters beinhalten (z. B. Kenntnisse und Fähigkeiten, Infrastruktur, wirtschaftliche Situation, unternehmensbezogener und aufsichtsrechtlicher Status). Gegebenenfalls kann das Unternehmen zur Unterstützung der bei der Due-Diligence-Prüfung gewonnenen Erkenntnisse Zertifizierungen auf der Grundlage von internationalen Standards, Prüfberichte anerkannter Dritter oder interne Prüfberichte heranziehen.

Leitlinie 10 – Vertraglich geregelte Anforderungen

36. Die Rechte und Pflichten des Unternehmens und die Rechte und Pflichten des Cloud-Anbieters sollten eindeutig zugeteilt und in einer schriftlichen Vereinbarung festgehalten werden.

37. Unbeschadet der Anforderungen nach Artikel 274 der Delegierten Verordnung sollte die schriftliche Vereinbarung, die bei der Auslagerung von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an einen Cloud-Anbieter zwischen dem Unternehmen und diesem Cloud-Anbieter geschlossen wird, Folgendes beinhalten:

a. eine klare Beschreibung der auszuführenden ausgelagerten Funktion (Cloud-Dienste, einschließlich der Art von Unterstützungsdiensten);

b. das Datum des Beginns und gegebenenfalls des Endes der Vereinbarung sowie die Kündigungsfristen für den Cloud-Anbieter und für das Unternehmen;

c. die gerichtliche Zuständigkeit und das für die Vereinbarung geltende Recht;

d. die finanziellen Pflichten der Parteien;

e. die Angabe, ob die Weiterauslagerung einer kritischen oder wichtigen operativen Funktion oder Tätigkeit (oder wesentlicher Teile der Funktion oder Tätigkeit) zulässig ist, und wenn ja, welchen Bedingungen die erhebliche Weiterauslagerung unterliegt (siehe Leitlinie 13);

f. den Standort bzw. die Standorte (d. h. Regionen oder Länder), in denen relevante Daten gespeichert und verarbeitet werden, (Standort von Rechenzentren) und die zu erfüllenden Bedingungen, einschließlich der Anforderung, das Unternehmen zu benachrichtigen, wenn der Dienstleister einen Standortwechsel beabsichtigt;

g. die Bedingungen für Zugänglichkeit, Verfügbarkeit, Integrität, Vertraulichkeit, Schutz und Sicherheit relevanter Daten, wobei die Spezifikation in Leitlinie 12 berücksichtigt werden sollte;

h. das Recht des Unternehmens, die Leistung des Cloud-Anbieters regelmäßig zu überwachen;

i. die vereinbarte Dienstleistungsgüte, die präzise quantitative und qualitative Leistungsziele umfassen sollte, um eine rechtzeitige Überwachung zu ermöglichen, sodass unverzüglich geeignete Korrekturmaßnahmen ergriffen werden können, wenn die vereinbarte Dienstleistungsgüte nicht erreicht wird;

j. die Berichtspflichten des Cloud-Anbieters gegenüber dem Unternehmen, ggf. einschließlich der Verpflichtungen, für die Sicherheitsfunktion und für Schlüsselfunktionen des Unternehmens relevante Berichte vorzulegen, z. B. Berichte über die interne Prüffunktion des Cloud-Anbieters;

k. die Angabe, ob der Cloud-Anbieter verpflichtet werden sollte, Versicherungen gegen bestimmte Risiken abzuschließen, sowie ggf. die Höhe der geforderten Versicherungsdeckung;

l. die Anforderungen, Notfallpläne einzuführen und zu erproben;

m. die Anforderung an den Cloud-Anbieter, dem Unternehmen, seinen Aufsichtsbehörden und etwaigen anderen Personen, die von dem Unternehmen bzw. den Aufsichtsbehörden benannt werden, Folgendes zu gestatten:

    i. uneingeschränkten Zugang zu allen relevanten Geschäftsräumen (Hauptsitzen und Betriebszentren), einschließlich des gesamten Spektrums an relevanten Einrichtungen, Systemen, Netzwerken, Informationen und Daten, die für die Ausführung der ausgelagerten Funktion eingesetzt werden, auch in Bezug auf zugehörige Finanzinformationen, auf Personal und auf die externen Prüfer des Cloud-Anbieters („Zugangsrechte“);

    ii. uneingeschränkte Rechte auf Kontrolle und Prüfung im Zusammenhang mit der Vereinbarung über Cloud-Outsourcing („Prüfungsrechte“), damit sie die Auslagerungsvereinbarung überwachen können und sicherstellen können, dass alle geltenden aufsichtsrechtlichen und vertraglichen Anforderungen eingehalten werden;

n. die Bestimmungen, mit denen sichergestellt wird, dass das Unternehmen seine Daten im Fall der Insolvenz, der Abwicklung oder der Einstellung der Geschäftstätigkeit des Cloud-Anbieters wiedererlangen kann.

Leitlinie 11 – Zugangs- und Prüfungsrechte

38. In der Vereinbarung über Cloud-Outsourcing sollten die tatsächliche Ausübung von Zugangs- und Prüfungsrechten durch das Unternehmen sowie die Möglichkeiten zur Kontrolle von Cloud-Diensten nicht eingeschränkt werden, damit das Unternehmen seinen aufsichtsrechtlichen Verpflichtungen nachkommen kann.

39. Das Unternehmen sollte seine Zugangs- und Prüfungsrechte ausüben, die Prüfhäufigkeit festlegen und die Bereiche und Dienstleistungen bestimmen, die auf der Grundlage eines risikobasierten Ansatzes zu prüfen sind, und sich dabei an Abschnitt 8 der von der EIOPA bereitgestellten Leitlinien zum Governance-System orientieren.

40. Bei der Festlegung von Häufigkeit und Umfang der Ausübung von Zugangs- und Prüfungsrechten sollte das Unternehmen prüfen, ob eine kritische oder wichtige operative Funktion oder Tätigkeit vom Cloud-Outsourcing betroffen ist; ferner sollten Art und Umfang der Risiken berücksichtigt werden, die dem Unternehmen aus den Vereinbarungen über Cloud-Outsourcing entstehen, wie auch Art und Umfang der Auswirkungen solcher Vereinbarungen auf das Unternehmen.

41. Wenn die Ausübung der Zugangs- und Prüfungsrechte oder die Anwendung bestimmter Prüfverfahren durch das Unternehmen ein Risiko für die Umgebung des Cloud-Anbieters und/oder eines anderen Kunden dieses Anbieters mit sich bringt (z. B. Auswirkungen auf Dienstleistungsgüte, Datenverfügbarkeit, Vertraulichkeitsaspekte), sollten das Unternehmen und der Cloud-Anbieter Alternativen vereinbaren, die dem Unternehmen ein vergleichbares Sicherheitsniveau und eine vergleichbare Dienstleistungsgüte bieten (z. B. die Aufnahme spezieller zu erprobender Kontrollen in einen speziellen Bericht bzw. eine spezielle Zertifizierung des Cloud-Anbieters).

42. Unbeschadet der Tatsache, dass die Verantwortung für die Tätigkeit ihrer Cloud-Anbieter letztlich bei den Unternehmen liegt, können Unternehmen auf Folgendes zurückgreifen, um Prüfressourcen effizienter einzusetzen und den Verwaltungsaufwand für den Cloud-Anbieter und seine Kunden zu verringern:

a. Zertifizierungen durch Dritte und externe oder interne Prüfberichte, die der Cloud-Anbieter bereitstellt;

b. Sammelprüfungen (pooled audits, d. h. Prüfungen, die gemeinsam mit anderen Kunden desselben Cloud-Anbieters durchgeführt werden) oder Sammelprüfungen, die ein von ihnen benannter Dritter durchführt.

43. Beim Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten sollten die Unternehmen das in Absatz 42 Buchstabe a genannte Verfahren nur anwenden,

a. um sicherzustellen, dass sich die Zertifizierung oder der Prüfbericht auf die Systeme (d. h. Prozesse, Anwendungen, Infrastruktur, Rechenzentren usw.) und auf die Kontrollen erstreckt, die das Unternehmen festgelegt hat, und dass dabei die Einhaltung der relevanten aufsichtsrechtlichen Anforderungen geprüft wird;

b. um den Inhalt neuer Zertifizierungen und Prüfberichte regelmäßig sorgfältig zu prüfen und um nachzuprüfen, dass die Zertifizierungen oder Berichte nicht veraltet sind;

c. um sicherzustellen, dass die zentralen Systeme und Kontrollen in künftigen Ausgaben der Zertifizierung oder des Prüfberichts berücksichtigt werden;

d. wenn sie sich vergewissert haben, dass die zertifizierende oder prüfende Stelle geeignet ist (beispielsweise in Bezug auf die Rotation des zertifizierenden oder

prüfenden Unternehmens, die Qualifikationen, das Fachwissen oder die neuerliche Prüfung/die Überprüfung der Nachweise in der zugrunde liegenden Prüfdatei);

e. wenn sie sich vergewissert haben, dass die Zertifizierungen und Prüfungen auf der Grundlage angemessener Standards erfolgen und einen Test der operativen Wirksamkeit der eingeführten zentralen Kontrollen beinhalten;

f. wenn sie das vertraglich geregelte Recht haben, die Erweiterung des Umfangs der Zertifizierungen oder Prüfberichte auf andere relevante Systeme und Kontrollen zu verlangen; Anzahl und Häufigkeit solcher Ersuchen um Änderungen des Umfangs sollten sich in einem vernünftigen Rahmen bewegen und unter dem Aspekt des Risikomanagements berechtigt sein;

g. wenn sie weiterhin das vertraglich geregelte Recht haben, nach eigenem Ermessen individuelle Vor-Ort-Prüfungen in Bezug auf das Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten durchzuführen; dieses Recht sollte bei besonderem Bedarf ausgeübt werden, dem durch andere Formen der Interaktion mit dem Cloud-Anbieter nicht entsprochen werden kann.

44. Beim Outsourcing von kritischen oder wichtigen operativen Funktionen an Cloud-Anbieter sollte das Unternehmen prüfen, ob Zertifizierungen durch Dritte und Berichte von Dritten gemäß Absatz 42 Buchstabe a angemessen und hinreichend sind, um ihren aufsichtsrechtlichen Pflichten nachzukommen; zudem sollten sie sich auf der Grundlage eines risikobasierten Ansatzes nicht dauerhaft ausschließlich auf diese Berichte und Zertifizierungen verlassen.

45. Vor einem geplanten Vor-Ort-Besuch sollte die Partei, die ihr Zugangsrecht ausübt, (Unternehmen, Prüfer oder Dritter, der im Namen des Unternehmens bzw. der Unternehmen tätig ist) ihren Besuch innerhalb einer angemessenen Frist ankündigen, es sei denn, ein Notfall oder eine Krisensituation lassen eine vorherige Ankündigung nicht zu. In der Ankündigung sollten unter anderem Ort und Zweck des Besuchs angegeben sowie die Teilnehmer an dem Besuch genannt werden.

46. In Anbetracht der Tatsache, dass Cloud-Lösungen technisch hochkomplex sind, sollte das Unternehmen nachprüfen, dass die Mitarbeiter, die die Prüfung durchführen – seien es die eigenen Prüfer, die Prüfergruppe, die in seinem Namen tätig ist, oder die vom Cloud-Anbieter benannten Prüfer – oder ggf. die Mitarbeiter, die die Zertifizierungen durch Dritte oder die Prüfberichte des Dienstleisters kontrollieren, über die entsprechenden Fähigkeiten und Kenntnisse verfügen, die für die Durchführung der relevanten Prüfungen und/oder Bewertungen erforderlich sind.

Leitlinie 12 – Sicherheit von Daten und Systemen

47. Das Unternehmen sollte sicherstellen, dass Cloud-Anbieter europäische und nationale Vorschriften sowie entsprechende IKT-Sicherheitsstandards einhalten.

48. Beim Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an Cloud-Anbieter sollte das Unternehmen in der Auslagerungsvereinbarung außerdem bestimmte Anforderungen an die Informationssicherheit festlegen und die Einhaltung dieser Anforderungen regelmäßig überwachen.

49. Für die Zwecke von Absatz 48 sollte das Unternehmen beim Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten an Cloud-Anbieter auf der Grundlage eines risikobasierten Ansatzes und unter Berücksichtigung seiner Zuständigkeiten und der Zuständigkeiten des Cloud-Anbieters Folgendes:

a. eine klare Verteilung fest umrissener Aufgaben und Zuständigkeiten in Bezug auf die operativen Funktionen und Tätigkeiten, die von dem Cloud-Outsourcing betroffen sind, zwischen dem Cloud-Anbieter und dem Unternehmen vereinbaren;

b. ein angemessenes Schutzniveau für vertrauliche Daten, die Kontinuität ausgelagerter Tätigkeiten sowie die Integrität und Rückverfolgbarkeit von Daten und Systemen im Rahmen des geplanten Cloud-Outsourcing festlegen und zur Vorgabe machen;

c. erforderlichenfalls für Daten bei der Übertragung, Daten im Speicher und ruhende Daten bestimmte Maßnahmen in Betracht ziehen, z. B. den Einsatz von Verschlüsselungstechnologien in Verbindung mit einem geeigneten Schlüsselmanagement;

d. Mechanismen für die Integration der Cloud-Dienste mit den Systemen des Unternehmens in Betracht ziehen, z. B. die Schnittstellen für die Anwendungsprogramme und ein zuverlässiges Verfahren für das Nutzer- und Zugangsmanagement;

e. vertraglich sicherstellen, dass die Verfügbarkeit von Netzkapazitäten und die zu erwartende Kapazität ggf. und soweit möglich hohe Kontinuitätsanforderungen erfüllen;

f. ordnungsgemäße Kontinuitätsanforderungen festlegen und zur Vorgabe machen, wobei ggf. für jede Stufe der Technologiekette angemessene Werte sichergestellt sein sollten;

g. ein zuverlässiges und gut dokumentiertes Incident-Management-Verfahren anwenden, bei dem unter anderem die jeweiligen Zuständigkeiten festgelegt sind, z. B. durch die Ausarbeitung eines Kooperationsmodells bei tatsächlichen oder mutmaßlichen Störungen;

h. einen risikobasierten Ansatz für den Standort bzw. die Standorte für die Speicherung und die Verarbeitung der Daten (z. B. Land oder Region) und für die Belange der Informationssicherheit annehmen;

i. die Erfüllung der Anforderungen an die Wirksamkeit und Effizienz von Kontrollmechanismen überwachen, die der Cloud-Anbieter im Hinblick auf die Verringerung der mit den erbrachten Dienstleistungen verbundenen Risiken eingeführt hat.

Leitlinie 13 – Weiterauslagerung von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten

50. Falls die Weiterauslagerung von kritischen oder wichtigen operativen Funktionen (oder Teilen der Funktionen) zulässig ist, sollte die Vereinbarung über Cloud-Outsourcing zwischen dem Unternehmen und dem Cloud-Anbieter Folgendes vorsehen:

a. Präzisierung aller Arten von Tätigkeiten, die von einer potenziellen Weiterauslagerung ausgeschlossen sind;

b. Angabe der Bedingungen, die bei einer Weiterauslagerung zu erfüllen sind (z. B. dass auch der Dienstleister, an den die Weiterauslagerung erfolgt, den entsprechenden Pflichten des Cloud-Anbieters in vollem Umfang nachkommt). Zu diesen Pflichten gehören die Prüf- und Zugangsrechte und die Sicherheit von Daten und Systemen;

c. Angabe, dass die umfassende Rechenschaftspflicht und die umfassende Kontrollpflicht in Bezug auf die weiterausgelagerten Dienstleistungen letztlich bei dem Cloud-Anbieter verbleiben;

d. Aufnahme einer Verpflichtung für denCloud-Anbieter, das Unternehmen über etwaige geplante erhebliche Änderungen bei den Unterauftragnehmern oder den weiterausgelagerten Dienstleistungen, die sich auf die Fähigkeit des Dienstleisters auswirken könnten, seinen Pflichten nach der Vereinbarung über Cloud-Outsourcing nachzukommen, zu informieren. Die Frist für die Benachrichtigung über solche Änderungen sollte so bemessen sein, dass das Unternehmen zumindest eine Risikobewertung der Auswirkungen der vorgeschlagenen Änderungen durchführen kann, bevor es zur tatsächlichen Änderung bei den Dienstleistern, an die Aufgaben weiterausgelagert wurden, oder bei den weiterausgelagerten Dienstleistungen kommt;

e. Gewährleistung, dass das Unternehmen in den Fällen, in denen ein Cloud-Anbieter bei einem Dienstleister, an den Aufgaben weiterausgelagert wurden, oder bei weiterausgelagerten Dienstleistungen Änderungen beabsichtigt, die sich nachteilig auf die Risikobewertung der vereinbarten Dienstleistungen auswirken würden, das Recht hat, Widerspruch gegen derartige Änderungen einzulegen und/oder den Vertrag zu beenden bzw. aus dem Vertrag auszusteigen.

Leitlinie 14 – Überwachung und Kontrolle von Vereinbarungen über Cloud-Outsourcing

51. Das Unternehmen sollte die Ausführung der Tätigkeiten, die Sicherheitsmaßnahmen und die Einhaltung der vereinbarten Dienstleistungsgüte durch seinen Cloud-Anbieter regelmäßig auf der Grundlage eines risikobasierten Ansatzes überwachen. Der Hauptschwerpunkt sollte auf dem Cloud-Outsourcing von kritischen und wichtigen operativen Funktionen liegen.

52. Zu diesem Zweck sollte das Unternehmen Überwachungs- und Kontrollmechanismen einführen, bei denen ggf. und soweit möglich berücksichtigt werden sollte, dass kritische oder wichtige operative Funktionen oder Teile der Funktionen weiterausgelagert wurden.

53. Das Verwaltungs-, Management- oder Aufsichtsorgan sollte in regelmäßigen Abständen auf den aktuellen Stand hinsichtlich der Risiken gebracht werden, die in Bezug auf das Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten ermittelt wurden.

54. Das Unternehmen sollte hinreichende Ressourcen mit angemessenen Fähigkeiten und Kenntnissen für die Überwachung der in die Cloud ausgelagerten Dienstleistungen einsetzen, um die angemessene Überwachung und Kontrolle seiner Vereinbarungen über Cloud-Outsourcing zu gewährleisten. Die Mitarbeiter des Unternehmens, die mit diesen Tätigkeiten beauftragt sind, sollten, soweit dies für notwendig erachtet wird, sowohl über Kenntnisse im IKT-Bereich als auch über Kenntnisse der Geschäftstätigkeit verfügen.

Leitlinie 15 – Kündigungsrechte und Ausstiegsstrategien

55. Beim Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten sollte das Unternehmen eine eindeutig formulierte Klausel bezüglich einer Ausstiegsstrategie, die ihm ggf. die Kündigung der Vereinbarung ermöglicht, in die Vereinbarung über Cloud-Outsourcing aufnehmen. Die Kündigung sollte

unbeschadet der Kontinuität und der Qualität der Dienstleistungserbringung des Unternehmens gegenüber den Versicherungsnehmern möglich sein. Zu diesem Zweck sollte das Unternehmen:

a. Ausstiegspläne entwickeln, die umfassend, dienstleistungsbasiert, dokumentiert und hinreichend erprobt sind (z. B. durch eine Analyse der potenziellen Kosten, Auswirkungen, Ressourcen und zeitlichen Auswirkungen der verschiedenen potenziellen Ausstiegsoptionen);

b. alternative Lösungen ermitteln sowie angemessene und machbare Übergangspläne erarbeiten, damit das Unternehmen in der Lage ist, bestehende Tätigkeiten und Daten von dem Cloud-Anbieter abzuziehen und auf alternative Dienstleister zu übertragen bzw. wieder in das Unternehmen zu integrieren. Bei diesen Lösungen sollten die Herausforderungen berücksichtigt werden, die sich aus dem Standort der Daten ergeben können, wobei die Maßnahmen ergriffen werden sollten, die erforderlich sind, um in der Übergangsphase Geschäftskontinuität sicherzustellen;

c. sicherstellen, dass der Cloud-Anbieter das Unternehmen bei der Übertragung der ausgelagerten Daten, Systeme oder Anwendungen an einen anderen Dienstleister oder direkt an das Unternehmen angemessen unterstützt;

d. mit dem Cloud-Anbieter vereinbaren, dass der Cloud-Anbieter die Daten des Unternehmens nach der Rückübertragung an das Unternehmen in allen Regionen vollständig und sicher löschen wird.

56. Bei der Ausarbeitung von Ausstiegsstrategien sollte das Unternehmen Folgendes berücksichtigen:

a. Festlegung der Ziele der Ausstiegsstrategie;

b. Festlegung der Ereignisse, die die Aktivierung der Ausstiegsstrategie auslösen könnten (z. B. anhand von zentralen Risikoindikatoren, die auf eine unannehmbare Dienstleistungsgüte hinweisen);

c. Durchführung einer Business-Impact-Analyse, die in einem angemessenen Verhältnis zu den ausgelagerten Tätigkeiten steht und Aussagen dazu liefern soll, welche personellen und sonstigen Ressourcen für die Umsetzung des Ausstiegsplans erforderlich wären und wie lange dies dauern würde;

d. Zuteilung von Aufgaben und Zuständigkeiten für die Abwicklung von Ausstiegsplänen und Übergangsmaßnahmen;

e. Festlegung von Erfolgskriterien für die Übertragung.

Leitlinie 16 – Beaufsichtigung von Vereinbarungen über Cloud-Outsourcing durch Aufsichtsbehörden

57. Die Aufsichtsbehörden sollten die Analyse der Auswirkungen, die sich aus Vereinbarungen des Unternehmens über Cloud-Outsourcing ergeben, im Rahmen ihres aufsichtsrechtlichen Überprüfungsverfahrens durchführen. Der Schwerpunkt der Analyse der Auswirkungen sollte insbesondere auf den Vereinbarungen liegen, die die Auslagerung kritischer oder wichtiger operativer Funktionen oder Tätigkeiten betreffen.

58. Die Aufsichtsbehörden sollten bei der Beaufsichtigung von Vereinbarungen von Unternehmen über Cloud-Outsourcing die folgenden Risiken berücksichtigen:

a. Risiken im IKT-Bereich;

b. sonstige operative Risiken (einschließlich rechtlicher Risiken und Risiken für die Einhaltung von Vorschriften, für die Auslagerungssteuerung und das Third-Party-Management);

c. Reputationsrisiko;

d. Konzentrationsrisiko einschließlich des Konzentrationsrisikos auf Länder-/Sektorebene.

59. Im Rahmen ihrer Prüfung sollten die Aufsichtsbehörden die folgenden Aspekte auf der Grundlage eines risikobasierten Ansatzes berücksichtigen:

a. Sind die Governance-Verfahren und die operativen Verfahren des Unternehmens für die Genehmigung, Umsetzung, Überwachung, Verwaltung und Verlängerung von Vereinbarungen über Cloud-Outsourcing angemessen und wirksam?

b. Verfügt das Unternehmen über hinreichende Ressourcen mit angemessenen Fähigkeiten und Kenntnissen für die Überwachung der in die Cloud ausgelagerten Dienstleistungen?

c. Ermittelt und steuert das Unternehmen alle in diesen Leitlinien hervorgehobenen Risiken?

60. Bei Gruppen sollte die Gruppenaufsicht sicherstellen, dass sich die Auswirkungen des Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten in der Risikobewertung für die Gruppenaufsicht niederschlagen, wobei die Anforderungen gemäß den Absätzen 58 und 59 und die individuellen Merkmale der Governance der Gruppe sowie die individuellen operativen Merkmale der Gruppe berücksichtigt werden.

61. Wenn das Cloud-Outsourcing von kritischen oder wichtigen operativen Funktionen oder Tätigkeiten mehrere Unternehmen in verschiedenen Mitgliedstaaten betrifft und die Muttergesellschaft oder eine Tochtergesellschaft (z. B. ein Unternehmen oder ein Dienstleistungsunternehmen der Gruppe, wie der IKT-Anbieter der Gruppe) die zentrale Verwaltung innehat, sollten die Gruppenaufsicht und/oder die entsprechenden Aufsichtsbehörden der Unternehmen, die an dem Cloud-Outsourcing beteiligt sind, im Kollegium der Aufsichtsbehörden ggf. erörtern, welche Auswirkungen das Cloud-Outsourcing auf das Risikoprofil der Gruppe hat.

62. Wenn Bedenken ermittelt werden, die zu der Schlussfolgerung führen, dass ein Unternehmen nicht mehr über fundierte Governance-Regelungen verfügt oder dass es die aufsichtsrechtlichen Anforderungen nicht erfüllt, sollten die Aufsichtsbehörden angemessene Maßnahmen ergreifen; hierzu kann z. B. gehören, von dem Unternehmen die Verbesserung der Governance-Regelung zu fordern, den Umfang der ausgelagerten Funktionen zu begrenzen oder einzuschränken oder den Ausstieg aus einer oder mehreren Auslagerungsvereinbarungen zu fordern. In Anbetracht der Notwendigkeit, die Kontinuität des Geschäftsbetriebs des Unternehmens sicherzustellen, könnte insbesondere die Stornierung von Verträgen verlangt werden, wenn Aufsicht und Durchsetzung aufsichtsrechtlicher Anforderungen durch andere Maßnahmen nicht gewährleistet werden können.

Regeln über die Einhaltung von Vorschriften und Berichterstattung

63. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1094/2010 herausgegeben wurden. Gemäß Artikel 16 Absatz 3 dieser Verordnung unternehmen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen, um diese Leitlinien und Empfehlungen zu berücksichtigen.

64. Die zuständigen Behörden, die diese Leitlinien berücksichtigen bzw. dies beabsichtigen, sollten sie in angemessener Weise in ihren Regulierungs- bzw. Aufsichtsrahmen integrieren.

65. Die zuständigen Behörden müssen der EIOPA innerhalb von zwei Monaten nach Erscheinen der übersetzten Fassungen bestätigen, dass sie diese Leitlinien berücksichtigen bzw. dies beabsichtigen, und die Gründe angeben, wenn sie die Leitlinien nicht berücksichtigen werden.

66. Geht innerhalb der genannten Frist keine Antwort ein, wird davon ausgegangen, dass die zuständigen Behörden ihrer Berichterstattungspflicht nicht nachkommen, und dies wird entsprechend erfasst.

Schlussbestimmung bezüglich der Überprüfung

67. Die vorliegenden Leitlinien unterliegen der Überprüfung durch die EIOPA.