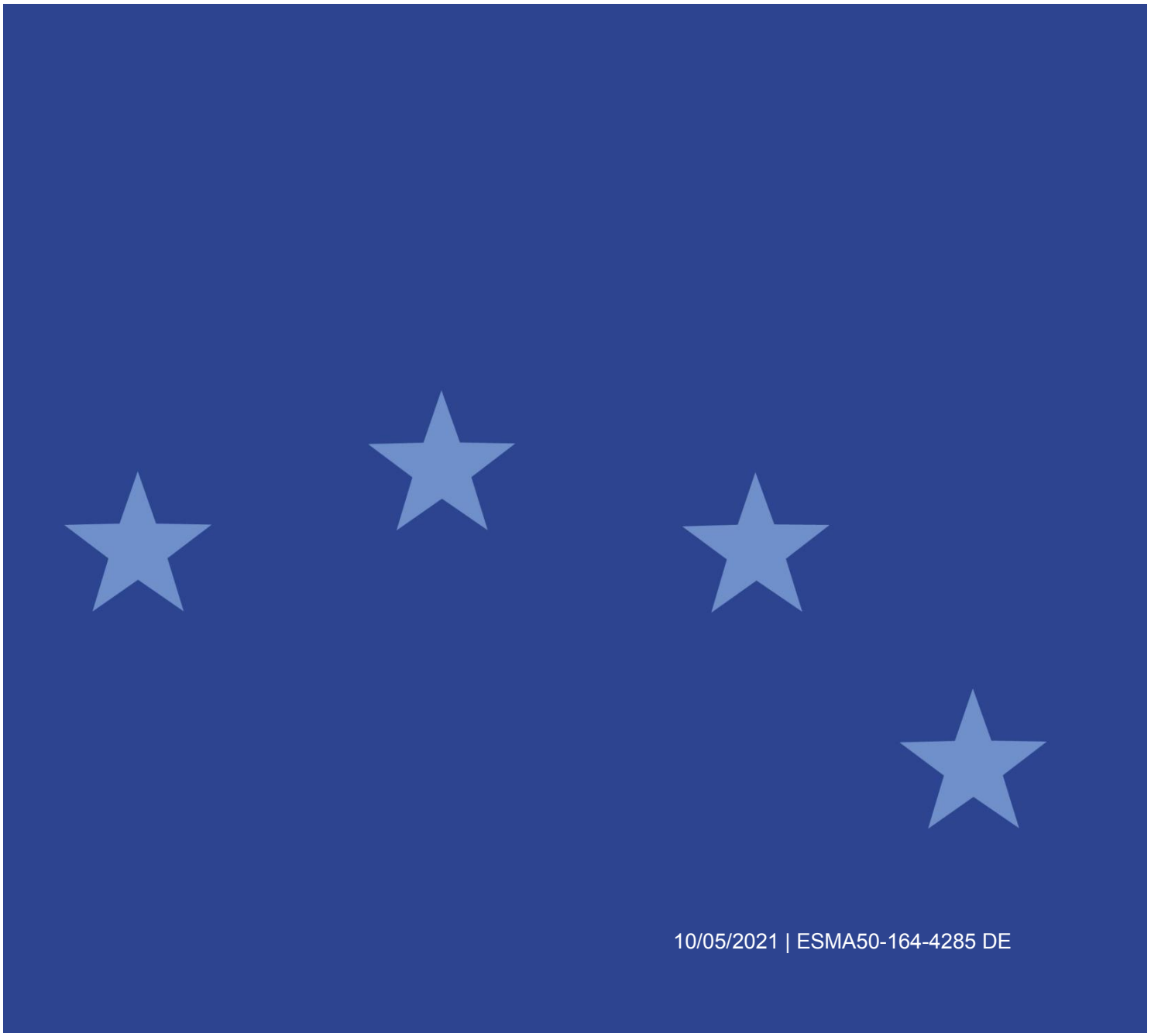
esma European Securities and Markets Authority

Leitlinien

zur Auslagerung an Cloud-Anbieter



10/05/2021 | ESMA50-164-4285 DE

Inhalt

I. Geltungsbereich 2
II. Rechtsrahmen, Abkürzungen und Begriffsbestimmungen 3
III. Zweck 10
IV. Einhaltung der Vorschriften und Berichtspflichten 10
V. Leitlinien zur Auslagerung an Cloud-Anbieter 11
Leitlinie 1. Governance, Kontrolle und Dokumentation 11
Leitlinie 2. Risikoanalyse der Auslagerung und Due-Diligence-Prüfung 13
Leitlinie 3. Zentrale Bestandteile des Vertrags 16
Leitlinie 4. Informationssicherheit 17
Leitlinie 5. Ausstiegsstrategien 19
Leitlinie 6. Zugangs- und Prüfungsrecht 20
Leitlinie 7. Sub-Auslagerungen 22
Leitlinie 8. Schriftliche Mitteilung an die zuständigen Behörden 23
Leitlinie 9. Überwachung von Auslagerungsvereinbarungen mit Cloud-Anbietern 24

I. Geltungsbereich

Für wen?

1. Diese Leitlinien richten sich an zuständige Behörden sowie an i) Verwalter alternativer Investmentfonds (AIFM) und Verwahrstellen alternativer Investmentfonds (AIF), ii) Organismen für gemeinsame Anlagen in Wertpapieren (OGAW), Verwaltungsgesellschaften und Verwahrstellen von OGAW und Investmentgesellschaften, die keine gemäß der OGAW-Richtlinie zugelassene Verwaltungsgesellschaft benannt haben, iii) zentrale Gegenparteien (CCP), einschließlich Tier-2-Drittstaaten-CCP, die die einschlägigen EMIR-Anforderungen erfüllen, iv) Transaktionsregister (TR), v) Wertpapierfirmen und Kreditinstitute im Rahmen der Erbringung von Wertpapierdienstleistungen und der Ausübung von Anlagetätigkeiten, Datenbereitstellungsdienste und Betreiber von Handelsplätzen, vi) Zentralverwahrer (CSD), vii) Ratingagenturen (CRA), viii) Verbriefungsregister und ix) Administratoren kritischer Referenzwerte.

2. Die ESMA zieht diese Leitlinien auch heran, wenn sie prüft, inwiefern eine Tier-2-Drittstaaten-CCP diesen Anforderungen entspricht, indem sie die in dem Drittstaat anwendbaren vergleichbaren Anforderungen erfüllt (siehe Artikel 25 Absatz 2b Buchstabe a der EMIR).

Was?

3. Diese Leitlinien beziehen sich auf die folgenden Bestimmungen:

   a) Artikel 15, 18, 20 und 21 Absatz 8 der AIFM-Richtlinie; Artikel 13, 22, 38, 39, 40, 44, 45, 57 Absatz 1 Buchstabe d, 57 Absatz 2, 57 Absatz 3, 58, 75, 76, 77, 79, 81, 82 und 98 der Delegierten Verordnung (EU) 2013/231 der Kommission;
   b) Artikel 12 Absatz 1 Buchstabe a, 13, 14 Absatz 1 Buchstabe c, 22, 22a, 23 Absatz 2, 30 und 31 der OGAW-Richtlinie; Artikel 4 Absätze 1 bis 3, 4 Absatz 5, 5 Absatz 2, 7, 9, 23 Absatz 4, 32, 38, 39 und 40 der Richtlinie 2010/43/EU der Kommission; Artikel 2 Absatz 2 Buchstabe j, 3 Absatz 1, 13 Absatz 2, 15, 16 und 22 der Delegierten Verordnung (EU) 2016/438 der Kommission;
   c) Artikel 25, 26 Absatz 1, 26 Absatz 3, 26 Absatz 6, 34, 35 und 78 bis 81 der EMIR; Artikel 5 und 12 der SFTR; Artikel 3 Absatz 1 Buchstabe f, 3 Absatz 2, 4, 7 Absatz 2 Buchstaben d und f, 9 und 17 der Delegierten Verordnung (EU) Nr. 153/2013 der Kommission; Artikel 16 und 21 der Delegierten Verordnung (EU) Nr. 150/2013 der Kommission; Artikel 16 und 21 der Delegierten Verordnung (EU) 2019/359 der Kommission;
   d) Artikel 16 Absatz 2, 16 Absatz 4, 16 Absatz 5, 18 Absatz 1, 19 Absatz 3 Buchstabe a, 47 Absatz 1 Buchstaben b und c, 48 Absatz 1, 64 Absatz 4, 65

Absatz 5 und 66 Absatz 31 der MiFID II; Artikel 21 Absätze 1 bis 3, 23, 29 Absatz 5, 30, 31 und 32 der Delegierten Verordnung (EU) 2017/565 der Kommission; Artikel 6, 15 und 16 Absatz 6 der Delegierten Verordnung (EU) 2017/584 der Kommission; Artikel 6, 7, 8 und 9 der Delegierten Verordnung (EU) 2017/571 der Kommission;

e) Artikel 22, 26, 30, 42, 44 und 45 der CSDR und Artikel 33, 47, 50 Absatz 1, 57 Absatz 2 Buchstabe i, 66, 68, 75, 76, 78 und 80 der Delegierten Verordnung (EU) 2017/392 der Kommission;
f) Artikel 9 und Anhang I, Abschnitt A Nummern 4 und 8 und Anhang II Nummer 17 der Verordnung über Ratingagenturen und Artikel 11 und 25 der Delegierten Verordnung (EU) 2012/449 der Kommission;
g) Artikel 10 Absatz 2 der Verbriefungsverordnung;
h) Artikel 6 Absätze 3 und 10 der Referenzwert-Verordnung und Anhang I Nummer 7 der Delegierten Verordnung (EU) 2018/1646 der Kommission.

Wann?

4. Diese Leitlinien gelten ab dem 31. Juli 2021 für alle Auslagerungsvereinbarungen mit Cloud-Anbietern, die an oder nach diesem Tag geschlossen, verlängert bzw. geändert werden. Die Firmen sollten bestehende Auslagerungsvereinbarungen mit Cloud-Anbietern überprüfen und entsprechend ändern, um sicherzustellen, dass sie diese Leitlinien ab dem 31. Dezember 2022 berücksichtigen. Wenn die Überprüfung von Auslagerungsvereinbarungen kritischer oder wesentlicher Funktionen an Cloud-Anbieter nicht bis zum 31. Dezember 2022 abgeschlossen ist, sollten die Firmen ihre zuständige Behörde entsprechend informieren und dabei die für die Fertigstellung der Überprüfung geplanten Maßnahmen oder die mögliche Ausstiegsstrategie angeben.

II. Rechtsrahmen, Abkürzungen und Begriffsbestimmungen

Rechtsrahmen

ESMA-Verordnung	Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission[2]
AIFM-Richtlinie	Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien

[1] Vom 1. Januar 2022 an gelten die Bezugnahmen auf Artikel 64 Absatz 4, 65 Absatz 5 und 66 Absatz 3 der MiFID II als Bezugnahmen auf Artikel 27g Absatz 4, 27h Absatz 5 und 27i Absatz 3 der MiFIR.
[2] ABl. L 331 vom 15.12.2010, S. 84.

	2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010[3]
Delegierte Verordnung (EU) Nr. 231/2013 der Kommission	Delegierte Verordnung (EU) Nr. 231/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates im Hinblick auf Ausnahmen, die Bedingungen für die Ausübung der Tätigkeit, Verwahrstellen, Hebelfinanzierung, Transparenz und Beaufsichtigung[4]
OGAW-Richtlinie	Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW)[5]
Richtlinie 2010/43/EU der Kommission	Richtlinie 2010/43/EU der Kommission vom 1. Juli 2010 zur Durchführung der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates im Hinblick auf organisatorische Anforderungen, Interessenkonflikte, Wohlverhalten, Risikomanagement und den Inhalt der Vereinbarung zwischen Verwahrstelle und Verwaltungsgesellschaft[6]
Delegierte Verordnung (EU) 2016/438 der Kommission	Delegierte Verordnung (EU) 2016/438 der Kommission vom 17. Dezember 2015 zur Ergänzung der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates in Bezug auf die Pflichten der Verwahrstellen[7]
EMIR	Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister[8]
SFTR	Verordnung (EU) 2015/2365 des Europäischen Parlaments und des Rates vom 25. November 2015 über die Transparenz von Wertpapierfinanzierungsgeschäften und der Weiterverwendung sowie zur Änderung der Verordnung (EU) Nr. 648/2012[9]
Delegierte Verordnung (EU) Nr. 153/2013 der Kommission	Delegierte Verordnung (EU) Nr. 153/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates in Bezug auf technische Regulierungsstandards für Anforderungen an zentrale Gegenparteien[10]

[3] ABl. L 174 vom 1.7.2011, S. 1.
[4] ABl. L 83 vom 22.3.2013, S. 1.
[5] ABl. L 302 vom 17.11.2009, S. 32.
[6] ABl. L 176 vom 10.7.2010, S. 42.
[7] ABl. L 78 vom 24.3.2012, S. 11.
[8] ABl. L 201 vom 27.7.2012, S. 1.
[9] ABl. L 337 vom 23.12.2015, S. 1.
[10] ABl. L 52 vom 23.2.2013, S. 41.

Delegierte Verordnung (EU) Nr. 150/2013 der Kommission	Delegierte Verordnung (EU) Nr. 150/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister durch technische Regulierungsstandards, in denen die Einzelheiten eines Antrags auf Registrierung als Transaktionsregister festgelegt werden[11]
Delegierte Verordnung (EU) 2019/359 der Kommission	Delegierte Verordnung (EU) 2019/359 der Kommission vom 13. Dezember 2018 zur Ergänzung der Verordnung (EU) 2015/2365 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards, in denen die Einzelheiten eines Antrags auf Registrierung oder Ausweitung der Registrierung als Transaktionsregister festgelegt werden[12]
MiFID II	Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU[13]
MiFIR	Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012[14]
Delegierte Verordnung (EU) 2017/565 der Kommission	Delegierte Verordnung (EU) 2017/565 der Kommission vom 25. April 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie[15]
Delegierte Verordnung (EU) 2017/584 der Kommission	Delegierte Verordnung (EU) 2017/584 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze[16]
Delegierte Verordnung (EU) 2017/571 der Kommission	Delegierte Verordnung (EU) 2017/571 der Kommission vom 2. Juni 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische

[11] ABl. L 52 vom 23.2.2013, S. 25.
[12] ABl. L 81 vom 22.3.2019, S. 45.
[13] ABl. L 173 vom 12.6.2014, S. 349.
[14] ABl. L 173 vom 12.6.2014, S. 84.
[15] ABl. L 87 vom 31.3.2017, S. 1.
[16] ABl. L 87 vom 31.3.2017, S. 350.

	Regulierungsstandards für die Zulassung, die organisatorischen Anforderungen und die Veröffentlichung von Geschäften für Datenbereitstellungsdienste[17]
CSDR	Verordnung (EU) Nr. 909/2014 vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012[18]
Delegierte Verordnung (EU) 2017/392 der Kommission	Delegierte Verordnung (EU) 2017/392 der Kommission vom 11. November 2016 zur Ergänzung der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Zulassung von und für aufsichtliche und operationelle Anforderungen an Zentralverwahrer[19]
Verordnung über Ratingagenturen	Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen[20]
Delegierte Verordnung (EU) Nr. 449/2012 der Kommission	Delegierte Verordnung (EU) Nr. 449/2012 der Kommission vom 21. März 2012 zur Ergänzung der Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates im Hinblick auf technische Regulierungsstandards für Informationen zur Registrierung und Zertifizierung von Ratingagenturen[21]
Verbriefungsverordnung	Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 zur Festlegung eines allgemeinen Rahmens für Verbriefungen und zur Schaffung eines spezifischen Rahmens für einfache, transparente und standardisierte Verbriefung und zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 648/2012[22]
Referenzwert-Verordnung	Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über Indizes, die bei Finanzinstrumenten und Finanzkontrakten als Referenzwert oder zur Messung der Wertentwicklung eines Investmentfonds verwendet werden, und zur Änderung der

[17] ABl. L 87 vom 31.3.2017, S. 126.
[18] ABl. L 257 vom 28.8.2014, S. 1.
[19] ABl. L 65 vom 10.3.2017, S. 48.
[20] ABl. L 302 vom 17.11.2009, S. 1.
[21] ABl. L 140 vom 30.5.2012, S. 32.
[22] ABl. L 347 vom 28.12.2017, S. 35.

	Richtlinien 2008/48/EG und 2014/17/EU sowie der Verordnung (EU) Nr. 596/2014[23]
Delegierte Verordnung (EU) 2018/1646 der Kommission	Delegierte Verordnung (EU) 2018/1646 der Kommission vom 13. Juli 2018 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur näheren Bestimmung der Angaben, die bei einem Antrag auf Zulassung und bei einem Antrag auf Registrierung vorzulegen sind[24]
DSGVO	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[25]

Abkürzungen

CSP	Cloud-Anbieter (*Cloud Service Provider*)
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
EU	Europäische Union

Begriffsbestimmungen

Funktion	bezeichnet alle Prozesse, Dienstleistungen oder Tätigkeiten;
Kritische oder wesentliche Funktion	bezeichnet jede Funktion, deren unzureichende oder unterlassene Wahrnehmung, zu einer wesentlichen Beeinträchtigung von Folgendem führen würde: a) der Einhaltung der Verpflichtungen einer Firma aus geltenden Rechtsvorschriften; b) der finanziellen Ergebnisse einer Firma,; oder c) der Solidität oder Kontinuität der zentralen Dienstleistungen und Tätigkeiten einer Firma
Cloud-Dienste	bezeichnet Dienstleistungen, die mithilfe von Cloud-Computing erbracht werden;

[23] ABl. L 171 vom 29.6.2016, S. 1.
[24] ABl. L 274 vom 5.11.2018, S. 43.
[25] ABl. L 119 vom 4.5.2016, S. 1-88.

Cloud-Computing oder Cloud[26]	bezeichnet ein Paradigma 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 einen Drittanbieter, der Cloud-Services im Rahmen einer Auslagerungsvereinbarung bereitstellt ;
Auslagerungsvereinbarung mit Cloud-Anbietern	bezeichnet eine Vereinbarung jeglicher Art, einschließlich Delegationsvereinbarungen, zwischen: (i) einer Firma und einem Cloud-Anbieter, in deren Rahmen dieser Cloud-Anbieter eine Funktion wahrnimmt, die die Firma sonst selbst wahrnehmen würde, oder (ii) einer Firma und einem Dritten, der kein Cloud-Anbieter ist, aber in erheblichem Maße auf einen Cloud-Anbieter zurückgreift, um eine Funktion wahrzunehmen, die die Firma sonst selbst wahrnehmen würde. In diesem Fall wird ein Verweis auf einen Cloud-Anbieter in diesen Richtlinien so verstanden werden, dass er sich auf einen solchen Dritten bezieht.
Sub-Auslagerung	bezeichnet eine Situation, in der der Cloud-Anbieter im Rahmen einer Auslagerungsvereinbarung die ausgelagerte Funktion (oder einen Teil dieser Funktion) an einen anderen Dienstleister weiter überträgt;
Cloud-Bereitstellungsmodell	bezeichnet die Art und Weise in welcher eine Cloud organisiert sein kann, bezogen auf die Kontrolle und die gemeinsame Nutzung von physischen oder virtuellen Ressourcen. Cloud-Bereitstellungsmodelle beinhalten Community-Clouds[27], Hybrid-Clouds[28], Private Clouds[29] und Public Clouds[30]

[26] Der Begriff „Cloud-Computing“ wird oft in abgekürzter Form als „Cloud“ bezeichnet. Um die Lektüre zu erleichtern, wird im Folgenden durchgängig der Begriff „Cloud“ verwendet.
[27] Ein Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich für eine bestimmte Gruppe von Kunden von Cloud-Diensten unterstützt werden und von dieser bestimmten Kundengruppe gemeinsam genutzt werden, wobei diese Kunden gemeinsame Anforderungen haben und untereinander in Beziehung stehen und die Ressourcen von mindestens einem Mitglied dieser Kundengruppe kontrolliert werden.
[28] Ein Cloud-Bereitstellungsmodell, das mindestens zwei verschiedene Cloud-Bereitstellungsmodelle nutzt.
[29] Ein Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich von einem einzigen Kunden von Cloud-Diensten genutzt werden und die Ressourcen von diesem Kunden kontrolliert werden.
[30] Ein Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste potenziell jedem Kunden von Cloud-Diensten zur Verfügung stehen und die Ressourcen vom Cloud-Anbieter kontrolliert werden.

Firmen

a) Verwalter alternativer Investmentfonds oder „AIFM“ im Sinne von Artikel 4 Absatz 1 Buchstabe b der AIFM-Richtlinie und Verwahrstellen gemäß Artikel 21 Absatz 3 der AIFM-Richtlinie (Verwahrstellen für alternative Investmentfonds);

b) Verwaltungsgesellschaften im Sinne von Artikel 2 Absatz 1 Buchstabe b der OGAW-Richtlinie (OGAW-Verwaltungsgesellschaften) und Verwahrstellen im Sinne von Artikel 2 Absatz 1 Buchstabe a der OGAW-Richtlinie (OGAW-Verwahrstellen);

c) zentrale Gegenparteien (CCP) im Sinne von Artikel 2 Absatz 1 der EMIR und Tier-2-Drittstaaten-CCP im Sinne von Artikel 25 Absatz 2a der EMIR, die die einschlägigen EMIR-Anforderungen gemäß Artikel 25 Absatz 2b Buchstabe a der EMIR erfüllen;

d) Transaktionsregister im Sinne von Artikel 2 Absatz 2 der EMIR und Artikel 3 Absatz 1 der SFTR;

e) Wertpapierfirmen im Sinne von Artikel 4 Absatz 1 Nummer 1 der MiFID II und Kreditinstitute im Sinne von Artikel 4 Absatz 1 Nummer 27 der MiFID II, die Wertpapierdienstleistungen und Anlagetätigkeiten im Sinne von Artikel 4 Absatz 1 Nummer 2 der MiFID II erbringen bzw. ausführen;

f) Datenbereitstellungsdienste im Sinne von Artikel 4 Absatz 1 Nummer 63 der MiFID II[31];

g) Marktbetreiber von Handelsplätzen im Sinne von Artikel 4 Absatz 1 Nummer 24 der MiFID II;

[31] Ab dem 1. Januar 2022 gilt die Bezugnahme auf diese Bestimmung als Bezugnahme auf Nummer 36a von Artikel 2 Absatz 1 der MiFIR.

h) Zentralverwahrer im Sinne von Artikel 2 Absatz 1 Nummer 1 der CSDR;

i) Ratingagenturen im Sinne von Artikel 3 Absatz 1 Buchstabe b der Verordnung über Ratingagenturen;

j) Verbriefungsregister im Sinne von Artikel 2 Absatz 23 der Verbriefungsverordnung;

k) Administrator kritischer Referenzwerte im Sinne von Artikel 3 Absatz 1 Nummer 25 der Referenzwert-Verordnung.

III. Zweck

5. Die vorliegenden Leitlinien basieren auf Artikel 16 Absatz 1 der ESMA-Verordnung. Ziel dieser Leitlinien ist es, innerhalb des Europäischen Finanzaufsichtssystems (ESFS) kohärente, effiziente und wirksame Aufsichtspraktiken festzulegen und sicherzustellen, dass in Fällen, in denen Firmen Auslagerungen an Cloud-Anbieter vornehmen, die in Abschnitt 1.1 unter der Überschrift „Was?“ genannten Anforderungen gemeinsam, einheitlich und kohärent erfüllt werden. Insbesondere sollen diese Leitlinien Firmen und zuständigen Behörden bei der Ermittlung, Bewältigung und Überwachung von Risiken und Herausforderungen im Zusammenhang mit Vereinbarungen über Auslagerungen an Cloud-Anbieter als Hilfestellung dienen, von der Auslagerungsentscheidung, der Wahl eines Cloud-Anbieters, der Überwachung ausgelagerter Tätigkeiten bis hin zur Berücksichtigung von Ausstiegsstrategien.

IV. Einhaltung der Vorschriften und Berichtspflichten

Status dieser Leitlinien

6. Gemäß Artikel 16 Absatz 3 der ESMA-Verordnung unternehmen die zuständigen Behörden und die Firmen alle erforderlichen Anstrengungen, um diesen Leitlinien nachzukommen.

7. Die von diesen Leitlinien betroffenen zuständigen Behörden sollten diesen Leitlinien nachkommen, indem sie sie ggf. in ihre nationalen Rechts- und/oder Aufsichtsrahmen übernehmen; und zwar auch dann, wenn bestimmte Leitlinien in erster Linie an Firmen gerichtet sind. In diesem Fall sollten die zuständigen Behörden durch ihre Aufsichtstätigkeit sicherstellen, dass die Firmen den Leitlinien nachkommen.

8. Im Rahmen ihrer ständigen direkten Aufsichtstätigkeit beurteilt die ESMA die Anwendung dieser Leitlinien durch Ratingagenturen, Transaktionsregister, Verbriefungsregister, Tier-2-Drittstaaten-CCP und ab dem 1. Januar 2022 auch durch Datenbereitstellungsdienste und Administratoren kritischer EU-Referenzwerte.

Berichtspflichten

9. Die zuständigen Behörden, für welche diese Leitlinien gelten, müssen die ESMA binnen zwei Monaten nach Veröffentlichung der Leitlinien auf der Website der ESMA in allen Amtssprachen der EU darüber unterrichten, ob sie den Leitlinien (i) nachkommen, (ii) nachzukommen beabsichtigen oder (iii) nicht nachkommen und nicht nachzukommen beabsichtigen.

10. Für den Fall der Nichteinhaltung müssen die zuständigen Behörden der ESMA zudem innerhalb von zwei Monaten ab dem Datum, an welchem die Leitlinien in allen Amtssprachen der EU auf der Website der ESMA veröffentlicht worden sind, die Gründe für die Nichteinhaltung der Leitlinien mitteilen. Eine Vorlage für entsprechende Mitteilungen steht auf der Website der ESMA zur Verfügung. Die ausgefüllte Vorlage ist an die ESMA zu senden.

11. Firmen sind nicht verpflichtet mitzuteilen, ob sie diesen Leitlinien nachkommen.

V. Leitlinien zur Auslagerung an Cloud-Anbieter

Leitlinie 1. Governance, Kontrolle und Dokumentation

12. Eine Firma sollte eine klare und aktuelle Strategie für Auslagerungen an Cloud-Anbieter haben, die mit den entsprechenden Strategien und internen Grundsätzen und Verfahren der Firma in Einklang steht und unter anderem die Bereiche Informations- und Kommunikationstechnologie, Informationssicherheit und operatives Risikomanagement abdeckt.

13. Eine Firma sollte:

    a) innerhalb ihrer Organisation eine klare Zuweisung der Zuständigkeiten für Dokumentation, Verwaltung und Kontrolle von Vereinbarungen über Auslagerungen an Cloud-Anbieter vornehmen,
    b) hinreichende Ressourcen zuteilen, um sicherzustellen, dass die vorliegenden Leitlinien eingehalten und alle anwendbaren rechtlichen Anforderungen bei Auslagerungsvereinbarungen mit Cloud-Anbietern erfüllt werden,
    c) eine Funktion für die Kontrolle von Auslagerungen an Cloud-Anbieter einrichten, oder leitende Angestellte benennen, die unmittelbar dem Leitungsorgan unterstellt sind und für das Risikomanagement und die Kontrolle der Risiken im Zusammenhang mit Vereinbarungen über Auslagerungen an Cloud-Anbieter

zuständig sind. Bei der Einhaltung dieser Leitlinien sollten die Firmen Art, Umfang und Komplexität ihrer Geschäftstätigkeit berücksichtigen, unter anderem im Hinblick auf das Risiko für das Finanzsystem und die den ausgelagerten Funktionen inhärenten Risiken; zudem sollten sie gewährleisten, dass ihr Leitungsorgan über die entsprechenden fachlichen Kompetenzen verfügt, um die Risiken verstehen zu können, die mit Vereinbarungen über Auslagerungen an Cloud-Anbieter verbunden sind.[32] Kleine und weniger komplexe Firmen sollten zumindest sicherstellen, dass eine klare Trennung der Aufgaben und Zuständigkeiten für die Verwaltung und Kontrolle von Vereinbarungen über Auslagerungen an Cloud-Anbieter besteht.

14. Eine Firma sollte die Ausführung von Tätigkeiten, die Sicherheitsmaßnahmen und die Einhaltung des vereinbarten Service Levels ihrer Cloud-Anbieter laufend überwachen. Diese Überwachungstätigkeit sollte risikobasiert sein, wobei ein besonderer Schwerpunkt auf den kritischen oder wesentlichen Funktionen liegen sollte, die ausgelagert wurden.

15. Eine Firma sollte in regelmäßigen Abständen und immer dann, wenn sich Risiko, Art oder Umfang einer ausgelagerten Funktion wesentlich geändert haben, überprüfen, ob ihre Vereinbarungen über Auslagerungen an Cloud-Anbieter eine kritische oder wesentliche Funktion betreffen.

16. Eine Firma sollte ein aktualisiertes Register mit Informationen über alle ihre Auslagerungsvereinbarungen mit Cloud-Anbietern führen und dabei zwischen Vereinbarungen über die Auslagerung von kritischen oder wesentlichen Funktionen und anderen Auslagerungsvereinbarungen unterscheiden. Bei der Unterscheidung zwischen der Auslagerung kritischer oder wesentlicher Funktionen und anderen Auslagerungsvereinbarungen sollte die Firma jeweils in einer knappen Zusammenfassung die Gründe angeben, warum die ausgelagerte Funktion als kritisch oder wesentlich gilt (bzw. warum nicht). Unter Berücksichtigung der nationalen Rechtsvorschriften sollte eine Firma über einen angemessenen Zeitraum auch ein Verzeichnis mit beendeten Vereinbarungen über Auslagerungen an Cloud-Anbieter führen.

17. Das Register sollte zu allen Auslagerungsvereinbarungen mit Cloud-Anbietern, die kritische oder wesentliche Funktionen betreffen, jeweils mindestens die folgenden Angaben enthalten:

    a) eine Referenznummer,
    b) das Datum des Inkrafttretens und ggf. das Datum der nächsten Vertragsverlängerung, das Enddatum und/oder die Kündigungsfristen, die für den Cloud-Anbieter und für die Firma gelten,
    c) eine Kurzbeschreibung der ausgelagerten Funktion einschließlich der Daten, die ausgelagert werden, mit der Angabe, ob diese Daten personenbezogene Daten

[32] Für Wertpapierfirmen und Kreditinstitute siehe: Gemeinsame Leitlinien der ESMA und der EBA zur Bewertung der Eignung von Mitgliedern des Leitungsorgans und Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU (EBA/GL/2017/12).

beinhalten (z. B. durch die Angabe „Ja“ oder „Nein“ in einem gesonderten Datenfeld),

d) eine von der Firma zugeordnete Kategorie, aus der die Art der ausgelagerten Funktion hervorgeht (z. B. Informationstechnologiefunktion, Kontrollfunktion) und anhand derer es möglich sein sollte, die verschiedenen Arten von Auslagerungsvereinbarungen mit Cloud-Anbietern zu identifizieren,
e) die Angabe, ob die ausgelagerte Funktion zeitkritische Geschäftsvorgänge unterstützt,
f) den Namen und (gegebenenfalls) den Markennamen des Cloud-Anbieters, das Land in dem er registriert ist, seine Unternehmensregistrierungsnummer, seine Rechtsträgerkennung (sofern vorhanden), seine eingetragene Anschrift, seine relevanten Kontaktdaten und den Namen seines Mutterunternehmens (falls vorhanden),
g) das auf die Auslagerungsvereinbarungen mit Cloud-Anbietern anwendbare Recht und ggf. die Wahl des Gerichtsstands,
h) die Art der Cloud-Dienste und die Bereitstellungsmodelle, die konkrete Art der zu speichernden Daten und die Standorte, an denen diese Daten gespeichert werden können (d. h. Regionen oder Länder),
i) das Datum der letzten Beurteilung der Kritikalität oder Wesentlichkeit der ausgelagerten Funktion und das Datum der nächsten geplanten Beurteilung,
j) das Datum der letzten Risikoanalyse/Prüfung des Cloud-Anbieters mit einer knappen Zusammenfassung der wichtigsten Ergebnisse und das Datum der nächsten geplanten Risikobewertung/Prüfung,
k) die Person bzw. das Entscheidungsgremium in der Firma, die bzw. das die Auslagerungsvereinbarungen mit Cloud-Anbietern genehmigt hat,
l) gegebenenfalls die Namen von Subunternehmen, an die eine kritische oder wesentliche Funktion (oder wesentliche Teile einer solchen Funktion) weiter ausgelagert wurde, einschließlich der Länder, in denen die Subunternehmen registriert sind und in denen die weiter ausgelagerte Dienstleistung erbracht wird, und der Standorte, an denen die Daten gespeichert werden (d. h. Regionen oder Länder),
m) die geschätzten jährlichen Kosten der Auslagerungsvereinbarungen mit Cloud-Anbietern.

18. Bei Auslagerungsvereinbarungen mit Cloud-Anbietern, die nicht kritische oder nicht wesentliche Funktionen betreffen, sollte eine Firma auf der Grundlage von Art, Umfang und Komplexität der mit der ausgelagerten Funktion verbundenen Risiken festlegen, welche Informationen in das Register aufzunehmen sind.

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

19. Vor dem Abschluss einer Auslagerungsvereinbarungen mit Cloud-Anbietern sollte eine Firma:

a) prüfen, ob die Auslagerungsvereinbarungen mit Cloud-Anbietern eine kritische oder wesentliche Funktion betrifft,

b) alle relevanten Risiken der Auslagerungsvereinbarungen mit Cloud-Anbietern ermitteln und bewerten,
c) eine angemessene Due-Diligence-Prüfung des künftigen Cloud-Anbieters durchführen,
d) etwaige Interessenkonflikte, die sich aus der Auslagerung ergeben könnten, ermitteln und beurteilen.

20. Die Risikoanalyse der Auslagerung und die Due-Diligence-Prüfung des künftigen Cloud-Anbieters sollten in einem angemessenen Verhältnis zu Art, Umfang und Komplexität der Funktion, die die Firma auszulagern beabsichtigt, und zu den inhärenten Risiken dieser Funktion stehen. Diese Prüfungen sollten zumindest eine Beurteilung der potenziellen Auswirkungen der Auslagerungsvereinbarungen mit Cloud-Anbietern auf die operationellen und rechtlichen Risiken der Firma, die Risiken für die Einhaltung der Vorschriften durch die Firma und die Reputationsrisiken der Firma umfassen.

21. Wenn die Auslagerungsvereinbarungen mit Cloud-Anbietern kritische oder wesentliche Funktionen betrifft, sollte eine Firma außerdem:

a) alle relevanten Risiken bewerten, die sich infolge der Auslagerungsvereinbarungen mit Cloud-Anbietern ergeben können, einschließlich der Risiken für Informations- und Kommunikationstechnologie, Informationssicherheit und Fortführung des Geschäftsbetriebs, der rechtlichen Risiken, der Risiken in Bezug auf die Einhaltung der Vorschriften, der Reputationsrisiken und der operationellen Risiken; zu berücksichtigen sind hierbei auch potenzielle Einschränkungen der Kontrolle für die Firma durch Folgendes:
   i. den gewählten Cloud-Anbieter und die vorgeschlagenen Bereitstellungsmodelle,
   ii. die Migration und/oder der Umsetzungsprozess,
   iii. die Sensibilität der Funktion und die zugehörigen Daten, die für die Auslagerung in Betracht gezogen werden, sowie die zu treffenden Sicherheitsmaßnahmen,
   iv. die Interoperabilität der Systeme und Anwendungen der Firma und des Cloud-Anbieters, d. h. ihre Kapazität in Bezug auf den Austausch von Informationen und die wechselseitige Nutzung der übermittelten Informationen,
   v. die Übertragbarkeit der Daten der Firma, d. h. die Fähigkeit, die Daten der Firma problemlos von einem Cloud-Anbieter an einen anderen oder zurück an die Firma zu übertragen,
   vi. die politische Stabilität, die Sicherheitslage und das Rechtssystem (einschließlich der geltenden Bestimmungen für die Rechtsdurchsetzung, der im Falle eines Konkurses des Cloud-Anbieters anwendbaren insolvenzrechtlichen Bestimmungen, der geltenden Datenschutzbestimmungen und der Bewertung, ob die Bedingungen für die Übermittlung personenbezogener Daten an Dritte gemäß der DSGVO erfüllt sind) in den Ländern (in oder außerhalb der EU), in denen die ausgelagerten Funktionen bereitgestellt und die ausgelagerten Daten

gespeichert würden; im Falle einer Sub-Auslagerung die zusätzlichen Risiken, die sich ergeben können, wenn der Subunternehmer in einem Drittstaat oder in einem anderen Land als der Cloud-Anbieter niedergelassen ist, und im Falle einer Sub-Auslagerungskette alle zusätzlichen Risiken, die sich unter anderem aus der Tatsache ergeben können, dass zwischen der Firma und dem Subunternehmer, der die ausgelagerte Funktion wahrnimmt, kein direkter Vertrag geschlossen wurde,

vii. eine potenzielle Konzentration innerhalb der Firma, (ggf. auch auf Gruppenebene) die sich aus dem Abschluss mehrerer Auslagerungsvereinbarungen an ein und denselben Cloud-Anbieter ergibt, sowie eine potenzielle Konzentration innerhalb des Finanzsektors der EU, die entsteht, wenn mehrere Auslagerungsvereinbarungen mit ein und demselben Cloud-Anbieter oder mit einer kleinen Gruppe von Cloud-Anbietern eingehen. Bei der Prüfung des Konzentrationsrisikos sollte die Firma alle ihre Auslagerungsvereinbarungen (und ggf. die Auslagerungsvereinbarungen auf Gruppenebene) mit dem betreffenden Cloud-Anbieter berücksichtigen,

b) die aus den Auslagerungsvereinbarungen mit Cloud-Anbietern erwarteten Vorteile und Kosten berücksichtigen; dies beinhaltet unter anderem die Abwägung etwaiger bedeutsamer Risiken, die verringert oder besser gesteuert werden können, gegen etwaige bedeutsame Risiken, die sich aus der Vereinbarung über Auslagerungen an Cloud-Anbieter ergeben können.

22. Falls kritische oder wesentliche Funktionen ausgelagert werden, sollte die Due-Diligence-Prüfung eine Bewertung der Eignung des Cloud-Anbieters beinhalten. Bei der Prüfung der Eignung des Cloud-Anbieters sollte eine Firma sicherstellen, dass der Cloud-Anbieter über die geschäftliche Reputation, die Kenntnisse und Fähigkeiten, die Mittel (unter anderem die personellen Mittel, die IT-Ressourcen und die finanziellen Mittel), die Organisationsstruktur und gegebenenfalls die entsprechende Zulassung oder Registrierung bzw. die entsprechenden Zulassungen oder Registrierungen verfügt, um die kritische oder wesentliche Funktion zuverlässig und professionell wahrnehmen zu können und um seinen Verpflichtungen während der Laufzeit der Auslagerungsvereinbarung mit dem Cloud-Anbieter nachkommen zu können. Zu den zusätzlichen Faktoren, die bei der Durchführung der Due-Diligence-Prüfung des Cloud-Anbieters zu berücksichtigen sind, gehören die folgenden Aspekte, wobei die Prüfung jedoch nicht hierauf beschränkt sein sollte:

a) Das Informationssicherheitsmanagement und insbesondere der Schutz personenbezogener, vertraulicher oder ansonsten sensibler Daten,
b) Die Serviceunterstützung einschließlich der Unterstützungspläne und der Ansprechpartner, sowie die Verfahren für das Störfallmanagement,
c) Die Pläne für die Fortführung des Geschäftsbetriebs und den Notfallsanierungsplan.

23. Eine Firma kann ggf. und zur Unterstützung der durchgeführten Due-Diligence-Prüfung auch auf Zertifizierungen nach internationalen Standards und auf externe oder interne Prüfberichte zurückgreifen.

24. Falls die Firma Kenntnis von wesentlichen Mängeln und/oder wesentlichen Veränderungen der erbrachten Dienstleistungen oder hinsichtlich der Situation des Cloud-Anbieters erlangt, sollte die Risikoanalyse der Auslagerung und die Due-Diligence-Prüfung des Cloud-Anbieters umgehend überprüft oder, wenn nötig, erneut durchgeführt werden.

25. Wenn eine Firma eine neue Vereinbarung mit einem Cloud-Anbieter schließt oder eine Vereinbarung mit einem Cloud-Anbieter, der bereits einer Prüfung unterzogen wurde, verlängert, sollte sie auf der Grundlage eines risikobasierten Ansatzes feststellen, ob eine neuerliche Due-Diligence-Prüfung erforderlich ist.

Leitlinie 3. Zentrale Bestandteile des Vertrags

26. Die jeweiligen Rechte und Pflichten einer Firma und ihres Cloud-Anbieters sollten in einer schriftlichen Vereinbarung klar festgehalten werden.

27. Die schriftliche Vereinbarung sollte ausdrücklich vorsehen, dass die Firma die Vereinbarung, wenn nötig, beenden kann.

28. Wenn kritische oder wesentliche Funktionen ausgelagert werden, sollte die schriftliche Vereinbarung zumindest die folgenden Elemente umfassen:

    a) eine klare Beschreibung der ausgelagerten Funktion,

    b) das Datum des Beginns und gegebenenfalls des Endes der Vereinbarung sowie die Kündigungsfristen für den Cloud-Anbieter und für die Firma,

    c) das auf die Vereinbarung anwendbare Recht und ggf. die Wahl des Gerichtsstands,

    d) die finanziellen Verpflichtungen der Firma und des Cloud-Anbieters,

    e) ob Sub-Auslagerungen zulässig sind und falls ja, unter welchen Bedingungen - unter Berücksichtigung der Leitlinie 7,

    f) den Standort bzw. die Standorte (d. h. Regionen oder Länder), an dem bzw. an denen die ausgelagerte Funktion ausgeübt wird und die Daten verarbeitet und gespeichert werden, und die einzuhaltenden Bestimmungen, einschließlich einer Bestimmung, dass die Firma zu benachrichtigen ist, wenn der Cloud-Anbieter einen Standortwechsel beabsichtigt,

    g) Bestimmungen in Bezug auf die Informationssicherheit und den Schutz personenbezogener Daten unter Berücksichtigung der Leitlinie 4,

    h) das Recht der Firma, die Leistungen des Cloud-Anbieters im Rahmen der Auslagerungsvereinbarung regelmäßig zu überwachen, unter Berücksichtigung der Leitlinie 6,

i) das vereinbarte Service Level, das unter anderem quantitative und qualitative Leistungsziele umfassen sollte, um eine rechtzeitige Überwachung zu ermöglichen, sodass unverzüglich geeignete Korrekturmaßnahmen ergriffen werden können, wenn das vereinbarte Service Level nicht erreicht wird,

j) die Berichtspflichten des Cloud-Anbieters gegenüber der Firma und ggf. die Verpflichtung Berichte vorzulegen, welche für die Sicherheitsfunktion und die Schlüsselfunktionen der Firma relevant sind, wie beispielsweise Berichte, die von der internen Revision des Cloud-Anbieters erstellt wurden,

k) Bestimmungen in Bezug auf das Störfallmanagement des Cloud-Anbieters, einschließlich der Verpflichtung des Cloud-Anbieters, der Firma unverzüglich Störfälle zu melden, die den Betrieb der von der Firma vertraglich übertragenen Dienstleistungen beeinträchtigt haben,

l) Angabe, ob der Cloud-Anbieter verpflichtet wird, für bestimmte Risiken eine Versicherung abzuschließen, sowie gegebenenfalls die Höhe der geforderten Versicherungsdeckung,

m) die Anforderungen an den Cloud-Anbieter, Pläne für die Fortführung des Geschäftsbetriebs und den Notfallsanierungsplan einzuführen und zu testen,

n) die Anforderung an den Cloud-Anbieter, der Firma, den zuständigen Behörden und allen anderen von der Firma oder den zuständigen Behörden benannten Personen das Recht auf Zugang („Zugangsrechte“) und auf Prüfung („Prüfungsrechte“) der entsprechenden Informationen, Räumlichkeiten, Systeme und Geräte des Cloud-Anbieters in dem für die Überwachung der Leistung des Cloud-Anbieters im Rahmen der Auslagerungsvereinbarung erforderlichen Umfang sowie der Einhaltung der anwendbaren gesetzlichen und vertraglichen Anforderungen durch den Cloud-Anbieter zu gewähren, unter Berücksichtigung der Leitlinie 6,

o) Bestimmungen, mit denen gewährleistet wird, dass die Daten, die der Cloud-Anbieter im Auftrag der Firma verarbeitet oder speichert, bei Bedarf abgerufen, wiederhergestellt und an die Firma zurückgegeben werden können, , unter Berücksichtigung der Leitlinie 5.

Leitlinie 4. Informationssicherheit

29. Eine Firma sollte in ihren internen Richtlinien und Verfahren sowie in der schriftlichen Auslagerungsvereinbarung mit dem Cloud-Anbieter Anforderungen an die Informationssicherheit festlegen und die Einhaltung dieser Anforderungen fortlaufend überwachen, einschließlich des Schutzes vertraulicher, personenbezogener oder anderweitig sensibler Daten. Diese Anforderungen sollten in einem angemessenen Verhältnis zu Art, Umfang und Komplexität der Funktion, die die Firma an den Cloud-Anbieter auslagert, und zu den mit dieser Funktion verbundenen Risiken stehen.

30. Zu diesem Zweck sollte eine Firma bei der Auslagerung von kritischen oder wesentlichen Funktionen auf der Grundlage eines risikobasierten Ansatzes und unbeschadet der anwendbaren Anforderungen nach der DSGVO zumindest Folgendes tun:

a) *Organisation der Informationssicherheit:* Sie sollte sicherstellen, dass eine klare Aufteilung der Aufgaben und Zuständigkeiten in Bezug auf die Informationssicherheit zwischen der Firma und dem Cloud-Anbieter erfolgt, die unter anderem die Erkennung von Bedrohungen, Störfallmanagement und Patch-Management betreffen, und dass der Cloud-Anbieter seine Aufgaben und Zuständigkeiten wirksam wahrnehmen kann.

b) *Identitäts- und Zugriffsverwaltung:* Sie sollte sicherstellen, dass wirksame Authentifizierungssysteme (z. B. Multifaktor-Authentifizierung) und Zugangskontrollen eingerichtet sind, um den unbefugten Zugang zu Daten und Backend-Cloudressourcen der Firma zu verhindern.

c) *Verschlüsselung und Schlüsselverwaltung:* Sie sollte sicherstellen, dass erforderlichenfalls entsprechende Verschlüsselungstechnologien für Daten bei der Übertragung, für gespeicherte Daten, Daten bei der Speicherung und Datensicherungen in Verbindung mit geeigneten Lösungen für das Schlüsselmanagement verwendet werden, um das Risiko eines unbefugten Zugangs zu den Verschlüsselungsschlüsseln einzugrenzen; insbesondere sollte die Firma bei der Wahl ihrer Schlüsselmanagementlösung auf dem neuesten Stand der Technik beruhende Technologie und entsprechende Verfahren in Betracht ziehen.

d) *Betriebs- und Netzwerksicherheit:* Sie sollte angemessene Ebenen der Netzwerkverfügbarkeit, Netzwerktrennung (z. B. Isolation von Mandanten in der gemeinsamen Umgebung der Cloud, operative Trennung in Bezug auf das Web, Anwendungslogik, Betriebssystem, Netzwerk, Datenbankmanagementsystem (DBMS) und Speicherebenen) und Verarbeitungsumgebungen (z. B. Erprobung, Erprobung der Nutzerakzeptanz, Entwicklung, Produktion) berücksichtigen.

e) *Anwendungsprogrammierschnittstellen (API):* Bei der Integration der Cloud-Dienste in die Systeme der Firma sind Mechanismen zu berücksichtigen, welche die Sicherheit der Anwendungsprogrammierschnittstellen (API) gewährleisten (z. B. Festlegung und Aufrechterhaltung von Richtlinien und Verfahren zur Informationssicherheit für APIs über mehrere Systemschnittstellen, Gerichtsbarkeiten und Geschäftsfunktionen hinweg, um eine unbefugte Offenlegung, Änderung oder Zerstörung von Daten zu verhindern).

f) *Geschäftskontinuität und Notfallsanierungsplan*: Sie sollte sicherstellen, dass wirksame Kontrollen hinsichtlich der Fortführung des Geschäftsbetriebs und des Notfallsanierungsplans vorhanden sind (z. B. Festlegung von Mindestkapazitätsanforderungen, Auswahl geografisch verteilter Hosting-Optionen mit der Möglichkeit, von einer zur anderen zu wechseln, oder die Anforderung und Überprüfung der Dokumentation, aus der der Übermittlungsweg der Daten der Firma zwischen den Systemen des Cloud-Anbieters hervorgeht, sowie die Berücksichtigung der Möglichkeit Machine Images an einen unabhängigen Speicherort zu kopieren, welcher vom Netzwerk ausreichend isoliert oder offline geschalten ist).

g) *Standort der Daten*: Sie sollte einen risikobasierten Ansatz für den Standort bzw. die Standorte (d. h. Regionen oder Länder) verfolgen, an dem/denen die Daten gespeichert und verarbeitet werden.

h) *Einhaltung und Überwachung der Vorschriften*: Sie sollte überprüfen, dass der Cloud-Anbieter international anerkannte Standards zur Informationssicherheit erfüllt und angemessene Kontrollen der Informationssicherheit eingerichtet hat (z. B. durch die Aufforderung an den Cloud-Anbieter, nachzuweisen, dass er entsprechende Überprüfungen der Informationssicherheit und regelmäßige Prüfungen und Tests der Informationssicherheitsmaßnahmen des Cloud-Anbieters durchführt).

Leitlinie 5. Ausstiegsstrategien

31. Bei der Auslagerung von kritischen oder wesentlichen Funktionen sollte eine Firma sicherstellen, dass sie die Auslagerungsvereinbarung mit dem Cloud-Anbieter beenden kann, 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. Zu diesem Zweck sollte eine Firma:

    a) umfassende, dokumentierte und hinreichend überprüfte Ausstiegspläne entwickeln. Diese Pläne sollten bei Bedarf aktualisiert werden, d. h. unter anderem bei Änderungen der ausgelagerten Funktion;
    b) alternative Lösungen ermitteln und Übergangspläneentwickeln, um die ausgelagerte Funktion und die entsprechenden Daten von dem Cloud-Anbieter und gegebenenfalls einem etwaigen Subunternehmer zurückzuholen und sie an einen von der Firma benannten alternativen Cloud-Anbieter oder direkt an die Firma zurück zu übertragen. 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 die Fortführung des Geschäftsbetriebs in der Übergangsphase sicherzustellen;
    c) sicherstellen, dass die schriftliche Auslagerungsvereinbarung mit dem Cloud-Anbieter eine Verpflichtung enthält, wonach der Cloud-Anbieter in dem Fall, dass die Firma die Ausstiegsstrategie einleitet, die geordnete Übergabe der ausgelagerten Funktion und der zugehörigen Datenverarbeitung von dem Cloud-Anbieter und einem etwaigen Subunternehmer an einen von der Firma benannten anderen Cloud-Anbieter oder direkt an die Firma unterstützen muss. Die Verpflichtung zur Unterstützung der geordneten Übergabe der ausgelagerten Funktion und der zugehörigen Datenverarbeitung sollte gegebenenfalls auch die sichere Löschung der Daten aus den Systemen des Cloud-Anbieters und eines etwaigen Subunternehmers beinhalten.

32. Bei der Entwicklung der unter a) und b) oben genannten Ausstiegspläne und -lösungen („Ausstiegsstrategie“) sollte die Firma folgendes tun:

    a) die Ziele der Ausstiegsstrategie festlegen;
    b) die auslösenden Ereignisse bestimmen, die die Einleitung der Ausstiegsstrategie zur Folge haben. Diese Ereignisse sollten zumindest die Beendigung der Auslagerungsvereinbarung mit dem Cloud-Anbieter auf Initiative der Firma oder

des Cloud-Anbieters und den Ausfall oder eine sonstige schwerwiegende Unterbrechung der Geschäftstätigkeit des Cloud-Anbieters beinhalten;

c) eine Business-Impact-Analyse durchführen, die in einem angemessenen Verhältnis zu der ausgelagerten Funktion steht und Aussagen dazu liefern soll, welche personellen und sonstigen Ressourcen für die Ausführung der Ausstiegsstrategie erforderlich wären;
d) Aufgaben und Verantwortlichkeiten für das Management der Ausstiegsstrategie zuweisen;
e) die Prüfung der Angemessenheit der Ausstiegsstrategie unter Verwendung eines risikobasierten Ansatzes (z. B. durch eine Analyse der potenziellen Kosten, Auswirkungen, Ressourcen und der zeitlichen Implikationen der Übertragung einer ausgelagerten Dienstleistung an einen anderen Anbieter);
f) Erfolgskriterien für die Übertragung festlegen.

33. Eine Firma sollte bei ihrer ständigen Überwachung und Kontrolle der vom Cloud-Anbieter im Rahmen der Auslagerungsvereinbarung erbrachten Dienstleistungen auch Indikatoren für die auslösenden Ereignisse berücksichtigen, die die Einleitung der Ausstiegsstrategie zur Folge haben.

Leitlinie 6. Zugangs- und Prüfungsrecht

34. Eine Firma sollte sicherstellen, dass die schriftliche Auslagerungsvereinbarung mit dem Cloud-Anbieter die wirksame Ausübung der Zugangs- und Prüfungsrechte sowie der Aufsichtsmöglichkeiten über den Cloud-Anbieter durch das Unternehmen und die zuständige Behörde nicht einschränkt.

35. Eine Firma sollte sicherstellen, dass bei der Ausübung der Zugangs- und Prüfungsrechte (z. B. in Bezug auf die Prüfungshäufigkeit und die zu prüfenden Bereiche und Dienstleistungen) berücksichtigt wird, ob die Auslagerung eine kritische oder wesentliche Funktion betrifft, und dass die Art und der Umfang der Risiken und der Auswirkungen, die sich aus der Auslagerungsvereinbarungen mit dem Cloud-Anbieter auf die Firma berücksichtigt sind.

36. Falls mit der Ausübung der Zugangs- und Prüfungsrechte oder mit der Anwendung bestimmter Prüfungstechniken ein Risiko für die Umgebung des Cloud-Anbieters und/oder eines anderen Kunden des Cloud-Anbieters verbunden ist (z. B. durch die Beeinträchtigung von Servicelevels, der Vertraulichkeit, Integrität und Verfügbarkeit von Daten), sollte der Cloud-Anbieter der Firma gegenüber klar begründen, warum dies ein Risiko darstellen würde; der Cloud-Anbieter sollte mit der Firma alternative Möglichkeiten vereinbaren, um ein vergleichbares Ergebnis zu erzielen (z. B. die Aufnahme bestimmter zu überprüfender Kontrollen in einen bestimmten Bericht des Cloud-Anbieters bzw. einer bestimmten Zertifizierung des Cloud-Anbieters).

37. Unbeschadet der Tatsache, dass die Verantwortung in Bezug auf die Auslagerungsvereinbarung mit dem Cloud-Anbieter letztlich bei den Firmen liegt, können Firmen auf Folgendes zurückgreifen, um Prüfungsressourcen effizienter zu

nutzen und um den organisatorischen Aufwand für den Cloud-Anbieter und seine Kunden zu verringern:

a) Zertifizierungen durch Dritte sowie externe oder interne Prüfberichte, die der Cloud-Anbieter zur Verfügung stellt,
b) Sammelprüfungen, die gemeinsam mit anderen Kunden desselben Cloud-Anbieters durchgeführt werden, oder Sammelprüfungen, die ein von mehreren Kunden desselben Cloud-Anbieters benannter externer Prüfer durchführt.

38. Bei der Auslagerung kritischer oder wesentlicher Funktionen sollte eine Firma prüfen, ob Zertifizierungen durch Dritte und externe oder interne Prüfberichte nach Punkt 37 Buchstabe a angemessen und ausreichend sind, um ihren Verpflichtungen aus den anwendbaren Rechtsvorschriften nachkommen zu können. Darüber hinaussollte die Firma bestrebt sein sich auf Dauer nicht ausschließlich auf solche Zertifizierungen und Berichte zu verlassen.

39. Bei der Auslagerung kritischer oder wesentlicher Funktionen sollte eine Firma nur dann auf Zertifizierungen durch Dritte sowie externe oder interne Prüfberichte nach Punkt 37 Buchstabe a zurückgreifen,

a) wenn sie sich vergewissert hat, dass der Umfang der Zertifizierungen oder der Prüfungsberichte die Schlüsselsysteme des CSP (z. B. Prozesse, Anwendungen, Infrastruktur, Rechenzentren), die von der Firma festgelegten zentralen Kontrollen und die Einhaltung der relevanten geltenden Rechtsvorschriften abdeckt,
b) wenn sie den Inhalt der Zertifizierungen oder der Prüfberichte regelmäßig sorgfältig prüft und sicherstellt, dass die Zertifizierungen oder Berichte nicht veraltet sind,
c) wenn sie sicherstellt, dass die Schlüsselsysteme und die zentralen Kontrollen des Cloud-Anbieters in künftigen Versionen der Zertifizierungen oder Prüfberichte berücksichtigt werden,
d) wenn sie mit der Zertifizierungs- oder Prüfstelle zufrieden ist (z. B. in Bezug auf ihre Qualifikationen, das Fachwissen, die Wiederholung / die Überprüfung der Fakten in den zugrunde liegenden Prüfunterlagen sowie der Rotation des Zertifizierungs- oder Prüfunternehmens),
e) wenn sie sich vergewissert hat, dass die Zertifizierungen und Prüfungen auf der Grundlage angemessener Standards erfolgen und einen Test der Wirksamkeit der eingeführten zentralen Kontrollen beinhalten,
f) wenn sie das vertraglich zugesicherte Recht hat, die Erweiterung des Umfangs der Zertifizierungen oder der Prüfberichte auf weitere relevante Systeme und Kontrollen des Cloud-Anbieters zu verlangen; die Anzahl und Häufigkeit solcher Ersuchen über Änderungen des Umfangs sollten aus Sichtweise des Risikomanagements angemessen und legitim sein.
g) wenn sie sich das vertragliche Recht vorbehält, nach eigenem Ermessen einzelne Vor-Ort-Prüfungen der ausgelagerten Funktion durchzuführen.

40. Eine Firma sollte sicherstellen, dass der Cloud-Anbieter innerhalb einer angemessenen Frist vor einem Vor-Ort-Besuch, auch vor einem solchen Besuch eines von der Firma benannten Dritten (z. B. eines Prüfers), vorab benachrichtigt wird, es sei

denn, eine frühzeitige vorherige Benachrichtigung ist aufgrund eines Notfalls oder einer Krisensituation nicht möglich oder würde dazu führen, dass die Prüfung nicht mehr wirksam wäre. In der Ankündigung sollten unter anderem Ort und Zweck des Besuchs angegeben werden, sowie die Mitarbeiter, die an dem Besuch teilnehmen werden.

41. In Anbetracht der Tatsache, dass sich Cloud-Dienste durch eine hohe technische Komplexität auszeichnen und dass sie besondere Herausforderungen hinsichtlich der Zuständigkeit mit sich bringen, sollten die Mitarbeiter, die die Prüfung durchführen – ob es sich nun um die internen Prüfer der Firma handelt oder um Prüfer, die im Auftrag der Firma tätig werden, – über die entsprechende Qualifikation und das entsprechende Wissen verfügen, um die relevanten Cloud-Dienste ordnungsgemäß bewerten und eine wirksame und sachgerechte Prüfung durchführen zu können. Dies sollte auch für die Mitarbeiter der Firmen gelten, die die Zertifizierungen oder Prüfberichte des Cloud-Anbieters überprüfen.

Leitlinie 7. Sub-Auslagerungen

42. Falls die Sub-Auslagerung von kritischen oder wesentlichen Funktionen (oder wesentlichen Teilen dieser Funktionen) zulässig ist, sollte die schriftliche Auslagerungsvereinbarung mit dem Cloud-Anbieter zwischen der Firma und dem Cloud-Anbieter Folgendes vorsehen:

    a) Angabe etwaiger Teile oder Aspekte der ausgelagerten Funktion, die von einer potenziellen Sub-Auslagerung ausgenommen sind;
    b) Angabe der im Fall einer Sub-Auslagerung zu erfüllenden Bedingungen;
    c) Angabe, dass der Cloud-Anbieter verantwortlich verbleibt und dass dieser verpflichtet ist, die von ihm an Subunternehmer weiter ausgelagerten Dienste zu überwachen, um sicherzustellen, dass alle vertraglichen Pflichten zwischen dem Cloud-Anbieter und der Firma kontinuierlich erfüllt werden;
    d) Aufnahme einer Verpflichtung des Cloud-Anbieters die Firma über eine etwaige beabsichtigte Sub-Auslagerung bzw. über wesentliche Änderungen einer solchen Sub-Auslagerung zu informieren, insbesondere in Fällen, in denen sich dies auf die Fähigkeit des Cloud-Anbieters auswirken könnte, seinen Verpflichtungen aus der Auslagerungsvereinbarung mit der Firma nachzukommen. Die in der schriftlichen Auslagerungsvereinbarung festgelegte Mitteilungsfrist sollte der Firma zumindest hinreichend Zeit gewähren, um eine Risikoanalyse der vorgeschlagenen Sub-Auslagerung oder wesentlicher Änderungen derselben durchzuführen und zu beanstanden oder ausdrücklich zu genehmigen, wie in Punkt (e) unten angegeben;
    e) Gewährleistung, dass die Firma berechtigt ist, der beabsichtigten Sub-Auslagerung oder den beabsichtigten wesentlichen Änderungen derselben zu widersprechen, oder dass eine ausdrückliche Zustimmung erteilt werden muss, bevor die vorgeschlagene Sub-Auslagerung oder die vorgeschlagenen wesentlichen Änderungen derselben vorgenommen werden;
    f) Gewährleistung, dass die Firma das vertraglich vereinbarte Recht hat, die Auslagerungsvereinbarung mit dem Cloud-Anbieter zu beenden, falls es der

vorgeschlagenen Sub-Auslagerung oder den vorgeschlagenen wesentlichen Änderungen derselben nicht zustimmt, oder falls eine Sub-Auslagerung an Subunternehmer zu Unrecht vorgenommen wurde (z. B. wenn der Cloud-Anbieter mit der Sub-Auslagerung fortfährt, ohne die Firma zu informieren, oder wenn er in schwerwiegender Weise gegen die in der Auslagerungsvereinbarung enthaltenen Bestimmungen für Sub-Auslagerungen verstößt).

43. Die Firma sollte sicherstellen, dass der Cloud-Anbieter eine angemessene Kontrolle über den Subunternehmer ausübt.

Leitlinie 8. Schriftliche Mitteilung an die zuständigen Behörden

44. Die Firma sollte ihre zuständige Behörde rechtzeitig schriftlich über beabsichtigte Auslagerungsvereinbarungen mit Cloud-Anbietern, die eine kritische oder wesentliche Funktion betreffen, informieren. Die Firma sollte ihre zuständige Behörde zudem rechtzeitig schriftlich über solche Auslagerungsvereinbarungen mit Cloud-Anbietern informieren, die eine Funktion betreffen, die zuvor als nicht kritisch oder nicht wesentlich eingestuft worden war, später jedoch kritisch oder wesentlich geworden ist.

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

    a) das Datum des Beginns der Auslagerungsvereinbarung mit dem Cloud-Anbieter und ggf. das Datum der nächsten Vertragsverlängerung, das Datum des Endes und/oder die Kündigungsfristen für den Cloud-Anbieter und die Firma;
    b) eine kurze Beschreibung der ausgelagerten Funktion;
    c) eine kurze Zusammenfassung der Gründe, weshalb die ausgelagerte Funktion als kritisch oder wesentlich gilt;
    d) den Namen und (gegebenenfalls) den Markennamen des Cloud-Anbieters, das Land, in dem er registriert ist, seine Unternehmensregistrierungsnummer, , seine Rechtsträgerkennung (sofern vorhanden), seine eingetragene Anschrift, seine relevanten Kontaktdaten und den Namen seines Mutterunternehmens (falls vorhanden);
    e) das auf die Auslagerungsvereinbarung mit dem Cloud-Anbieter anwendbare Recht und ggf. die Wahl des Gerichtsstands;
    f) die Bereitstellungsmodelle der Cloud-Dienste und die spezifische Art der beim Cloud-Anbieter befindlichen Daten und die Standorte, an denen diese Daten gespeichert werden (d. h. Regionen oder Länder);
    g) das Datum der letzten Bewertung der Kritikalität oder Wesentlichkeit der ausgelagerten Funktion;
    h) das Datum der letzten Risikoanalyse oder Prüfung des Cloud-Anbieters mit einer Kurzzusammenfassung der wichtigsten Ergebnisse und das Datum der nächsten geplanten Risikobewertung oder Prüfung;
    i) die Person bzw. das Entscheidungsgremium in der Firma, die bzw. das die Auslagerungsvereinbarung mit dem Cloud-Anbieter genehmigt hat;
    j) gegebenenfalls die Namen etwaiger Subunternehmer, an die wesentliche Teile einer kritischen oder wesentlichen Funktion weiter ausgelagert werden,

einschließlich des Landes oder der Region, in dem bzw. in der die Subunternehmer registriert sind, die ausgelagerten Dienste erbracht und die Daten gespeichert werden.

Leitlinie 9. Überwachung von Auslagerungsvereinbarungen mit Cloud-Anbietern

46. Die zuständigen Behörden sollten im Rahmen ihres Aufsichtsverfahrens die Risiken bewerten, die sich aus Vereinbarungen der Firmen über Auslagerungen an Cloud-Anbieter ergeben. Der besondere Schwerpunkt sollte hierbei auf den Vereinbarungen liegen, die die Auslagerung kritischer oder wesentlicher Funktionen betreffen.

47. Die zuständigen Behörden sollten sich vergewissern, dass sie eine wirksame Aufsicht ausüben können, insbesondere in Fällen, in denen die Firmen kritische oder wesentliche Funktionen auslagern, die dann außerhalb der EU durchgeführt werden.

48. Die zuständigen Behörden sollten auf der Grundlage eines risikobasierten Ansatzes prüfen, ob die Firmen:

    a) die entsprechende Governance, die entsprechenden Ressourcen und operativen Verfahren eingerichtet haben, um Auslagerungsvereinbarungen mit Cloud-Anbietern in angemessener und wirksamer Weise ein-gehen, um-setzen und kontrollieren zu können;
    b) alle relevanten Risiken der Auslagerungsvereinbarungen mit Cloud-Anbietern ermitteln und bewerten.

49. Bei der Feststellung von Konzentrationsrisiken sollten die zuständigen Behörden die Entwicklung dieser Risiken überwachen und sowohl ihre potenziellen Auswirkungen auf andere Firmen, die ihrer Aufsicht unterliegen, als auch auf die Stabilität des Finanzmarkts bewerten.