EBA/GL/2019/02

25. Februar 2019

Leitlinien zu Auslagerungen

1. Einhaltung und Meldepflichten

Status dieser Leitlinien

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

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Zuständige Behörden im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010 sollten für sie geltende Leitlinien in geeigneter Weise (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) in ihre Praktiken integrieren, einschließlich der Leitlinien, die in erster Linie an Institute und Zahlungsinstitute gerichtet sind.

Meldepflichten

3. In Übereinstimmung mit Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden die EBA bis zum ([TT.MM.JJJJ]) unterrichten, dass sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen bzw. andernfalls die Nichteinhaltung begründen. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2019/02“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

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

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

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand

5. In diesen Leitlinien werden die internen Governance-Regelungen, einschließlich eines soliden Risikomanagements, festgelegt, die Institute, Zahlungsinstitute und E-Geld-Institute einführen sollten, wenn sie Funktionen auslagern, insbesondere mit Blick auf die Auslagerung kritischer oder wesentlicher Funktionen.

6. In den Leitlinien wird festgelegt, wie die im vorstehenden Absatz genannten Regelungen von den zuständigen Behörden im Rahmen des Artikels 97 der Richtlinie 2013/36/EU [2], des Prozesses der aufsichtlichen Überprüfung und Bewertung (SREP), des Artikels 9 Absatz 3 der Richtlinie (EU) 2015/2366[3] und des Artikels 5 Absatz 5 der Richtlinie 2009/110/EG[4] überprüft und überwacht werden sollten, indem sie ihrer Pflicht nachkommen, die kontinuierliche Einhaltung der Zulassungsbedingungen der Institute, an die diese Leitlinien gerichtet sind, zu überwachen.

Adressaten

7. Diese Leitlinien richten sich an die zuständigen Behörden im Sinne des Artikels 4 Absatz 1 Ziffer 40 der Verordnung (EU) Nr. 575/2013[5], einschließlich der Europäischen Zentralbank in Zusammenhang mit der Wahrnehmung der ihr durch die Verordnung (EU) Nr. 1024/2013[6] übertragenen Aufgaben, an Institute im Sinne von Artikel 4 Absatz 1 Ziffer 3 der Verordnung (EU) Nr. 575/2013, an Zahlungsinstitute im Sinne des Artikels 4 Absatz 4 der Richtlinie (EU) 2015/2366 und an E-Geld-Institute im Sinne des Artikels 2 Absatz 1 der Richtlinie 2009/110/EG. Kontoinformationsdienstleister, die ausschließlich den Dienst im Sinne von Anhang I Nummer 8 der Richtlinie (EU) 2015/2366 erbringen, fallen in Übereinstimmung mit Artikel 33 derselben Richtlinie nicht in den Anwendungsbereich dieser Leitlinien.

---

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

[3] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

[4] Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG.

[5] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

[6] Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank.

8. Für die Zwecke dieser Leitlinien umfasst jeder Verweis auf „Zahlungsinstitute“ auch „E-Geld-Institute“ und jeder Verweis auf „Zahlungsdienste“ die „Ausgabe von E-Geld“.

Anwendungsbereich

9. Unbeschadet der Richtlinie 2014/65/EU[7] und der Delegierten Verordnung (EU) 2017/565 der Kommission[8] (die Anforderungen bezüglich der Auslagerung durch Institute enthält, die Wertpapierdienstleistungen erbringen und Anlagetätigkeiten ausüben, einschließlich der von der Europäischen Wertpapier- und Marktaufsichtsbehörde herausgegebenen Weisungen zu Wertpapierdienstleistungen und Anlagetätigkeiten) sollten die Institute im Sinne von Artikel 3 Absatz 1 Nummer 3 der Richtlinie 2013/36/EU diesen Leitlinien auf Einzel-, teilkonsolidierter und konsolidierter Basis nachkommen. Die zuständigen Behörden können Institute gemäß Artikel 21 der Richtlinie 2013/36/EU oder Artikel 109 Absatz 1 der Richtlinie 2013/36/EU in Verbindung mit Artikel 7 der Verordnung (EU) Nr. 575/2013 von der Anwendung auf Einzelbasis befreien. In Übereinstimmung mit Artikel 21 und den Artikeln 108 bis 110 der Richtlinie 2013/36/EU sollten Institute, die der Richtlinie 2013/36/EU unterliegen, der genannten Richtlinie und diesen Leitlinien auf konsolidierter und teilkonsolidierter Basis nachkommen.

10. Unbeschadet des Artikels 8 Absatz 3 der Richtlinie (EU) 2015/2366 und des Artikels 5 Absatz 7 der Richtlinie 2009/110/EG sollten Zahlungsinstitute und E-Geld-Institute diesen Leitlinien auf Einzelbasis nachkommen.

11. Die zuständigen Behörden, die für die Beaufsichtigung der Institute, Zahlungsinstitute und E-Geld-Institute verantwortlich sind, sollten diesen Leitlinien nachkommen.

Begriffsbestimmungen

12. Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU, der Verordnung (EU) Nr. 575/2013, der Richtlinie 2009/110/EG, der Richtlinie (EU) 2015/2366 und den EBA-Leitlinien zur internen Governance[9] verwendeten und definierten Begriffe in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

[7] 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 (ABl. L 173 vom 12.6.2014, S. 349).

[8] 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 (ABl. L 87 vom 31.3.2017, S. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

Auslagerung	Bezeichnet eine Vereinbarung gleich welcher Form zwischen einem Institut, einem Zahlungsinstitut oder einem E-Geld-Institut und einem Dienstleister, in deren Rahmen der Dienstleister einen Prozessdurchführt, eine Dienstleistung erbringt oder eine Tätigkeit ausführt, die das Institut, das Zahlungsinstitut oder das E-Geld-Institut ansonsten selbst übernähme.
Funktion	Bezeichnet jegliche Prozesse, Dienstleistungen oder Tätigkeiten.
Kritische oder wesentliche Funktion[10]	Bezeichnet jede Funktion, die gemäß Abschnitt 4 dieser Leitlinien als kritisch oder wesentlich gilt.
Weiterverlagerungen	Bezeichnet eine Situation, in der der Dienstleister im Rahmen einer Auslagerungsvereinbarung eine ausgelagerte Funktion an einen anderen Dienstleister weiter überträgt.[11]
Dienstleister	Bezeichnet einen Dritten, der im Rahmen einer Auslagerungsvereinbarung ein ausgelagertes Verfahren oder Teile eines solchen durchführt, eine ausgelagerte Dienstleistung oder Teile einer solchen erbringt oder eine ausgelagerte Tätigkeit oder Teile einer solchen ausführt.
Cloud-Dienste	Bezeichnet Dienste, die mithilfe von Cloud-Computing erbracht werden, d.h. 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 Interaktion des Dienstleisters bereitstellen lässt.
Öffentliche Cloud	Bezeichnet eine Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann.
Private Cloud	Bezeichnet eine Cloud-Infrastruktur, die ausschließlich von einem einzelnen Institut oder Zahlungsinstitut genutzt werden kann.
Community-Cloud	Bezeichnet eine Cloud-Infrastruktur, die ausschließlich von einer konkreten Instituts-

[10] Die Formulierung „kritische oder wesentliche Funktion“ beruht auf dem Wortlaut in der Richtlinie 2014/65/EU (MiFID II) und der Delegierten Verordnung (EU) 2017/565 der Kommission zur Ergänzung der MiFID II und wird ausschließlich für Zwecke der Auslagerung verwendet; sie bezieht sich nicht auf die Definition von „kritischen Funktionen“ für Zwecke des Sanierungs- und Abwicklungsrahmens, die in Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU (BRRD) enthalten ist.

[11] Für die Bewertung gelten die Bestimmungen des Abschnitts 3; in anderen EBA-Dokumenten wird auf eine weitere Auslagerung auch als „Auslagerungskette“ oder „Auslagerung im Kettenverfahren“ (*chain of outsourcing* bzw. *chain-outsourcing*) Bezug genommen.

	oder Zahlungsinstitutsgemeinschaft genutzt werden kann, einschließlich mehrerer Institute einer einzelnen Gruppe.
Hybrid-Cloud	Bezeichnet eine Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.
Leitungsorgan	Bezeichnet das Organ oder die Organe eines Instituts oder Zahlungsinstituts, das (die) nach nationalem Recht bestellt wurde (wurden) und befugt ist (sind), Strategie, Ziele und Gesamtpolitik des Instituts oder Zahlungsinstituts festzulegen und die Entscheidungen der Geschäftsleitung zu kontrollieren und zu überwachen, und dem die Personen, die die Geschäfte des Instituts oder Zahlungsinstituts tatsächlich führen, sowie die Geschäftsleiter und die für die Geschäftsleitung des Instituts zuständigen Personen angehören.

3. Umsetzung

Umsetzungsfrist

13. Mit Ausnahme von Absatz 63 Buchstabe b gelten diese Leitlinien ab dem 30. September 2019 für sämtliche Auslagerungsvereinbarungen, die an oder nach diesem Tag abgeschlossen, überprüft oder geändert werden. Absatz 63 Buchstabe b gilt ab dem 31. Dezember 2021.

14. Die Institute und Zahlungsinstitute sollten bestehende Auslagerungsvereinbarungen entsprechend überprüfen und ändern, um sicherzustellen, dass diese mit den vorliegenden Leitlinien in Einklang stehen.

15. In Fällen, in denen die Überprüfung von Auslagerungsvereinbarungen für kritische oder wesentliche Funktionen bis zum 31. Dezember 2021 nicht abgeschlossen ist, sollten die Institute und Zahlungsinstitute ihre zuständige Behörde über diesen Umstand informieren, wobei die für den Abschluss der Überprüfung geplanten Maßnahmen oder die mögliche Ausstiegsstrategie anzugeben sind.

Übergangsbestimmungen

16. Die Institute und Zahlungsinstitute sollten die Dokumentation aller bestehenden Auslagerungsvereinbarungen mit Ausnahme von Auslagerungsvereinbarungen mit Cloud-Anbietern in Übereinstimmung mit diesen Leitlinien nach dem ersten Verlängerungstermin jeder bestehenden Auslagerungsvereinbarung abschließen, spätestens jedoch bis zum 31. Dezember 2021.

Aufhebung

17. Die Leitlinien des Ausschusses der Europäischen Bankaufsichtsbehörden (CEBS) zum Outsourcing vom 14. Dezember 2006 und die Empfehlungen der EBA zur Auslagerung an Cloud-Anbieter[12] werden mit Wirkung zum 30. September 2019 aufgehoben.

[12] Empfehlungen zur Auslagerung an Cloud-Anbieter (EBA/REC/2017/03).

4. Leitlinien zu Auslagerungen

Titel I – Verhältnismäßigkeit: gruppenweite Anwendung und institutsbezogene Sicherungssysteme

1 Verhältnismäßigkeit

18. Die Institute, Zahlungsinstitute und zuständigen Behörden sollten bei der Einhaltung dieser Leitlinien bzw. der Überwachung der Einhaltung dieser Leitlinien den Grundsatz der Verhältnismäßigkeit berücksichtigen. Mit dem Grundsatz der Verhältnismäßigkeit soll sichergestellt werden, dass Governance-Regelungen, auch im Zusammenhang mit Auslagerungen, mit dem individuellen Risikoprofil, der Art und dem Geschäftsmodell des Instituts oder Zahlungsinstituts sowie dem Umfang und der Komplexität seiner Tätigkeiten in Einklang stehen, sodass die Ziele der regulatorischen Anforderungen wirksam erreicht werden.

19. Bei der Anwendung der in diesen Leitlinien festgelegten Anforderungen sollten die Institute und Zahlungsinstitute die Komplexität der ausgelagerten Funktionen, die mit der Auslagerungsvereinbarung verbundenen Risiken, die Kritikalität oder Wesentlichkeit der ausgelagerten Funktion sowie die potenziellen Folgen der Auslagerung auf die Kontinuität ihrer Tätigkeiten berücksichtigen.

20. Bei Anwendung des Grundsatzes der Verhältnismäßigkeit sollten die Institute, Zahlungsinstitute[13] und zuständigen Behörden die in Titel I der EBA-Leitlinien zur internen Governance in Einklang mit Artikel 74 Absatz 2 der Richtlinie 2013/36/EU festgelegten Kriterien berücksichtigen.

2 Auslagerung durch Gruppen und Institute, die Mitglieder eines institutsbezogenen Sicherungssystems sind

21. Gemäß Artikel 109 Absatz 2 der Richtlinie 2013/36/EU sollten diese Leitlinien unter Berücksichtigung des aufsichtlichen Konsolidierungskreises auch auf teilkonsolidierter und konsolidierter Basis Anwendung finden.[14] Zu diesem Zweck sollten die EU-Mutterunternehmen bzw. das Mutterunternehmen in einem Mitgliedstaat sicherstellen, dass die Governance-

[13] Die Zahlungsinstitute sollten auch die EBA-Leitlinien gemäß der PSD2 zu den Informationen, die für die Zulassung von Zahlungsinstituten und E-Geld-Instituten sowie für die Eintragung von Kontoinformationsdienstleistern zu übermitteln sind, berücksichtigen. Diese sind auf der Website der EBA unter folgendem Link verfügbar: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[14] Siehe Artikel 4 Absatz 1 Unterabsätze 47 und 48 der Verordnung (EU) Nr. 575/2013 hinsichtlich des Konsolidierungskreises.

Regelungen, Verfahren und Mechanismen in ihren Tochterunternehmen, einschließlich der Zahlungsinstitute, konsistent, gut integriert und für die wirksame Anwendung dieser Leitlinien auf allen maßgeblichen Ebenen angemessen sind.

22. Die Institute und Zahlungsinstitute gemäß Absatz 21 sowie Institute, die als Mitglieder eines institutsbezogenen Sicherungssystems zentral bereitgestellte Governance-Regelungen verwenden, sollten folgende Anforderungen erfüllen:

    a. Wenn diese Institute oder Zahlungsinstitute Auslagerungsvereinbarungen mit Dienstleistern innerhalb der Gruppe oder des institutsbezogenen Sicherungssystems geschlossen haben,[15] bleibt das Leitungsorgan dieser Institute oder Zahlungsinstitute auch weiterhin in vollem Umfang für die Erfüllung aller regulatorischen Anforderungen und die wirksame Anwendung dieser Leitlinien verantwortlich;

    b. Wenn diese Institute oder Zahlungsinstitute die operationellen Aufgaben der internen Kontrollfunktionen für die Überwachung und Prüfung der Auslagerungsvereinbarungen an einen Dienstleister innerhalb der Gruppe oder des institutsbezogenen Sicherungssystems auslagern, sollten die Institute sicherstellen, dass die betreffenden operationellen Aufgaben auch für diese Auslagerungsvereinbarungen wirksam wahrgenommen werden, einschließlich einer angemessenen Berichterstattung.

23. Zusätzlich zu Absatz 22 sollten Institute und Zahlungsinstitute innerhalb einer Gruppe, für die keine Ausnahmeregelung gemäß Artikel 109 der Richtlinie 2013/36/EU und Artikel 7 der Verordnung (EU) Nr. 575/2013 gewährt wurde, sowie Institute, die eine Zentralorganisation sind oder einer Zentralorganisation ständig zugeordnet sind, für die keine Ausnahmeregelung gemäß Artikel 21 der Richtlinie 2013/36/EU gewährt wurde, oder Institute, die Mitglied eines institutsbezogenen Sicherungssystems sind, Folgendes berücksichtigen:

    a. In Falle einer zentralisierten operativen Überwachung der Auslagerung (z. B. im Zuge einer Rahmenvereinbarung über die Überwachung von Auslagerungsvereinbarungen) sollten die Institute und Zahlungsinstitute sicherstellen, dass mindestens für ausgelagerte kritische oder wesentliche Funktionen sowohl eine unabhängige Überwachung des Dienstleisters als auch eine geeignete Kontrolle durch jedes Institut oder Zahlungsinstitut möglich ist, einschließlich einer mindestens jährlich bzw. auf Aufforderung erfolgenden Vorlage von Berichten der zentralisierten Überwachungsfunktion, die mindestens eine Zusammenfassung der Risikobewertung und Leistungsüberwachung umfassen. Darüber hinaus sollten die Institute und Zahlungsinstitute von der zentralisierten Überwachungsfunktion eine Zusammenfassung der einschlägigen Prüfungsberichte für kritische oder wesentliche Auslagerungen sowie auf Aufforderung den vollständigen Prüfungsbericht erhalten.

[15] In Einklang mit Artikel 113 Absatz 7 CRR bezeichnet ein institutsbezogenes Sicherungssystem eine vertragliche oder satzungsmäßige Haftungsvereinbarung, durch die die Institute, die Mitglied des Systems sind, abgesichert werden und insbesondere bei Bedarf ihre Liquidität und Solvenz sichergestellt wird, um einen Konkurs zu vermeiden.

b. Die Institute und Zahlungsinstitute sollten sicherstellen, dass ihr Leitungsorgan ordnungsgemäß über relevante geplante Änderungen bezüglich der zentral überwachten Dienstleister und die potenziellen Auswirkungen dieser Änderungen auf die kritischen oder wesentlichen Funktionen informiert wird, einschließlich einer Zusammenfassung der Risikoanalyse unter Einbeziehung rechtlicher Risiken, der Einhaltung von regulatorischen Anforderungen und der Auswirkungen auf die Dienstleistungsgüte, um ihm die Bewertung der Auswirkungen dieser Änderungen zu ermöglichen.

c. Wenn diese Institute und Zahlungsinstitute innerhalb einer Gruppe, einer Zentralorganisation zugeordnete Institute oder Institute, die Teil eines institutsbezogenen Sicherungssystems sind, sich vor dem Abschluss von Auslagerungsvereinbarungen wie in Abschnitt 12 dargelegt auf eine zentrale Bewertung dieser Auslagerungsvereinbarungen stützen, sollte jedes Institut und Zahlungsinstitut eine Zusammenfassung der Bewertung erhalten und sicherstellen, dass seine spezifische Struktur und seine besonderen Risiken im Rahmen des Entscheidungsprozesses berücksichtigt werden.

d. Wenn das in Abschnitt 11 beschriebene Register aller bestehenden Auslagerungsvereinbarungen zentral innerhalb einer Gruppe oder eines institutsbezogenen Sicherungssystems eingerichtet und geführt wird, sollten die zuständigen Behörden sowie alle Institute und Zahlungsinstitute ihr individuelles Register ohne größere Verzögerung erhalten können. Dieses Register sollte alle Auslagerungsvereinbarungen enthalten, einschließlich der Auslagerungsvereinbarungen mit Dienstleistern innerhalb der betreffenden Gruppe oder des betreffenden institutsbezogenen Sicherungssystems.

e. Wenn sich diese Institute und Zahlungsinstitute auf einen Ausstiegsplan für eine kritische oder wesentliche Funktion stützen, der auf Gruppenebene, innerhalb des institutsbezogenen Sicherungssystems oder von der Zentralorganisation festgelegt wurde, sollten alle Institute und Zahlungsinstitute eine Zusammenfassung des Plans erhalten und der Überzeugung sein, dass der Plan wirksam ausgeführt werden kann.

24. Sofern Ausnahmeregelungen gemäß Artikel 21 der Richtlinie 2013/36/EU oder Artikel 109 Absatz 1 der Richtlinie 2013/36/EU in Verbindung mit Artikel 7 der Verordnung (EU) Nr. 575/2013 gewährt wurden, sollten die Bestimmungen dieser Leitlinien vom Mutterunternehmen in einem Mitgliedstaat für sich selbst und für seine Tochterunternehmen bzw. von der Zentralorganisation und den ihr zugeordneten Instituten insgesamt angewendet werden.

25. Institute und Zahlungsinstitute, die Tochterunternehmen eines EU-Mutterunternehmens oder eines Mutterunternehmens in einem Mitgliedstaat sind, dem keine Ausnahmeregelung gemäß Artikel 21 der Richtlinie 2013/36/EU oder Artikel 109 Absatz 1 der Richtlinie 2013/36/EU in

Verbindung mit Artikel 7 der Verordnung (EU) Nr. 575/2013 gewährt wurde, sollten sicherstellen, dass sie diesen Leitlinien auf Einzelbasis nachkommen.

Titel II – Bewertung von Auslagerungsvereinbarungen

3 Auslagerung

26. Die Institute und Zahlungsinstitute sollten feststellen, ob eine Vereinbarung mit einem Dritten unter die Definition einer Auslagerung fällt. Im Rahmen dieser Bewertung sollte berücksichtigt werden, ob die an einen Dienstleister ausgelagerte Funktion (oder ein Teil von ihr) wiederkehrend oder laufend von dem Dienstleister wahrgenommen wird und ob diese Funktion (oder ein Teil derselben) normalerweise in den Anwendungsbereich der Funktionen fallen würde, der realistischerweise von Instituten oder Zahlungsinstituten wahrgenommen würden oder wahrgenommen werden könnten, selbst wenn das Institut oder das Zahlungsinstitut diese Funktion in der Vergangenheit nicht selbst wahrgenommen hat.

27. Wenn eine Vereinbarung mit einem Dienstleister mehrere Funktionen betrifft, so sollten die Institute und Zahlungsinstitute im Rahmen ihrer Bewertung alle Aspekte der Vereinbarung berücksichtigen; wenn z. B. die erbrachte Dienstleistung sowohl die Bereitstellung von Hardware für die Datenspeicherung als auch die Sicherung von Daten umfasst, sollten diese beiden Aspekte gemeinsam betrachtet werden.

28. Grundsätzlich sollten die Institute und Zahlungsinstitute folgende Fälle nicht als Auslagerung betrachten:

    a. eine Funktion, die aufgrund von Rechtsvorschriften von einem Dienstleister wahrzunehmen ist, z. B. Abschlussprüfungen;

    b. Marktinformationsdienste (z. B. Bereitstellung von Daten durch Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. globale Netzinfrastrukturen (z. B. Visa, MasterCard);

    d. Clearing- und Abwicklungsvereinbarungen zwischen Clearingstellen, zentralen Gegenparteien und Abwicklungsstellen sowie ihren Mitgliedern;

    e. globale Nachrichteninfrastrukturen zur Übermittlung von Zahlungsverkehrsdaten, die der Aufsicht durch einschlägige Behörden unterliegen;

    f. Korrespondenzbankdienstleistungen und

    g. den Erwerb von Dienstleistungen, die anderenfalls nicht vom Institut oder Zahlungsinstitut erbracht würden (z. B. Beratung durch einen Architekten, Bereitstellung eines Rechtsgutachtens und Vertretung vor Gericht und Verwaltungsbehörden, Reinigung, Gartenarbeiten und Instandhaltung der

Räumlichkeiten des Instituts oder Zahlungsinstituts, medizinische Dienstleistungen, Wartung von Firmenwagen, Verpflegungsdienste, Automatenservices, Bürodienstleistungen, Reisedienstleistungen, Poststellendienste, Rezeptionskräfte, Sekretariatskräfte und Telefonisten), von Waren (z. B. Plastikkarten, Kartenlesegeräte, Büromaterial, Computer, Möbel) oder Versorgungsleistungen (z. B. Strom, Gas, Wasser, Telefon).

4 Kritische oder wesentliche Funktionen

29. In folgenden Fällen sollten die Institute oder Zahlungsinstitute eine Funktion stets als kritisch oder wesentlich betrachten:[16]

    a. wenn eine unzureichende oder unterlassene Wahrnehmung der Funktion zu einer wesentlichen Beeinträchtigung von Folgendem führen würde:

        i. der kontinuierlichen Einhaltung der Zulassungsbedingungen oder sonstigen Pflichten gemäß der Richtlinie 2013/36/EU, der Verordnung (EU) Nr. 575/2013, der Richtlinie 2014/65/EU, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG und ihrer regulatorischen Pflichten;

        ii. ihrer finanziellen Ergebnisse oder

        iii. der Solidität oder Kontinuität ihrer Bank- und Zahlungsdienste und -geschäfte;

    b. bei der Auslagerung operationeller Aufgaben von internen Kontrollfunktionen, es sei denn, bei der Bewertung wurde festgestellt, dass eine unterlassene oder unzureichende Wahrnehmung der ausgelagerten Funktion keine negativen Auswirkungen auf die Wirksamkeit der internen Kontrollfunktion nach sich ziehen würde;

    c. wenn beabsichtigt wird, Funktionen des Bankgeschäfts oder der Zahlungsdienste in einem Umfang auszulagern, für den gemäß Abschnitt 12.1 eine Zulassung[17] einer zuständigen Behörde erforderlich wäre.

30. Bei Instituten ist auf die Bewertung der Kritikalität oder Wesentlichkeit von Funktionen besondere Aufmerksamkeit zu legen, wenn die Auslagerung Funktionen in Zusammenhang mit den Kerngeschäftsbereichen und kritischen Funktionen im Sinne von Artikel 2 Absatz 1 Unterabsatz 35 und Artikel 2 Absatz 1 Unterabsatz 36 der Richtlinie 2014/59/EU[18] betrifft, die

[16] Siehe auch Artikel 30 der Delegierten 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.

[17] Siehe die in Anhang I der Richtlinie 2013/36/EU aufgeführten Tätigkeiten.

[18] Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der

von den Instituten unter Zugrundelegung der Kriterien in den Artikeln 6 und 7 der Delegierten Verordnung (EU) 2016/778 der Kommission ermittelt wurden.[19] Funktionen, die für die Durchführung der Tätigkeiten von Kerngeschäftsbereichen oder kritischen Funktionen erforderlich sind, sollten für die Zwecke dieser Leitlinien als kritische oder wesentliche Funktionen angesehen werden, sofern das Institut nicht im Zuge seiner Bewertung feststellt, dass eine unterlassene oder unzureichende Wahrnehmung der ausgelagerten Funktion zu keinen negativen Auswirkungen auf die Geschäftskontinuität des Kerngeschäftsbereichs oder der kritischen Funktion führen würde.

31. Bei der Bewertung, ob sich eine Auslagerungsvereinbarung auf eine Funktion bezieht, die kritisch oder wesentlich ist, sollten die Institute und Zahlungsinstitute zusammen mit dem Ergebnis der in Abschnitt 12.2 beschriebenen Risikobewertung mindestens die folgenden Faktoren berücksichtigen:

    a. den Umstand, ob die Auslagerungsvereinbarung unmittelbar mit der Erbringung von Bankgeschäften oder Zahlungsdiensten verknüpft ist,[20] für die sie zugelassen sind;

    b. die potenziellen Auswirkungen einer Störung der ausgelagerten Funktion oder eines Versäumnisses des Dienstleisters, die Dienstleistung mit der vereinbarten Dienstleistungsgüte fortlaufend zu erbringen, auf

        i. ihre kurz- und langfristige finanzielle Widerstandsfähigkeit und Tragfähigkeit, gegebenenfalls einschließlich ihrer Vermögenswerte, ihres Kapitals, ihrer Kosten, Finanzierung, Liquidität, Gewinne und Verluste;

        ii. ihre Geschäftsfortführung und ihre operationelle Widerstandsfähigkeit;

        iii. ihr operationelles Risiko, einschließlich (Fehl-)Verhaltensrisiken, Informations- und Kommunikationstechnologie (IT)-Risiken und rechtlicher Risiken;

        iv. Reputationsrisiken;

        v. gegebenenfalls die Sanierungs- und Abwicklungsplanung, Abwicklungsfähigkeit und Fortführung des Geschäftsbetriebs bei einer Frühinterventionsmaßnahme, einem Sanierungs- oder einem Abwicklungsfall;

    c. die potenziellen Auswirkungen der Auslagerungsvereinbarung auf ihre Fähigkeit,

Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (BRRD) (ABl. L 173 vom 12.6.2014, S. 190).

[19] Delegierte Verordnung (EU) 2016/778 der Kommission vom 2. Februar 2016 zur Ergänzung der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates in Bezug auf die Umstände und Bedingungen, unter denen die Entrichtung von außerordentlichen nachträglich erhobenen Beiträgen teilweise oder vollständig aufgeschoben werden kann, und auf die Kriterien für die Bestimmung der Tätigkeiten, Dienstleistungen und Geschäfte im Zusammenhang mit „kritischen Funktionen“ und zur Präzisierung der Kriterien für die Bestimmung der Geschäftsbereiche und damit verbundenen Dienste im Zusammenhang mit den Kerngeschäftsbereichen (ABl. L 131 vom 20.5.2016, S. 41).

[20] Siehe die in Anhang I der Richtlinie 2013/36/EU aufgeführten Tätigkeiten.

i. sämtliche Risiken zu ermitteln, zu überwachen und zu steuern;

ii. sämtliche gesetzlichen und regulatorischen Anforderungen zu erfüllen;

iii. angemessene Prüfungen bezüglich der ausgelagerten Funktion durchzuführen;

d. die potenziellen Auswirkungen auf die für ihre Kunden erbrachten Dienstleistungen;

e. sämtliche Auslagerungsvereinbarungen, die aggregierte Risikoposition des Instituts oder Zahlungsinstituts gegenüber dem betreffenden Dienstleister und die potenziellen kumulativen Auswirkungen der Auslagerungsvereinbarungen in dem betreffenden Geschäftsbereich;

f. die Größe und die Komplexität des betroffenen Geschäftsbereichs;

g. die Möglichkeit einer eventuellen Ausweitung der vorgesehenen Auslagerungsvereinbarung, ohne dass die zugrunde liegende Vereinbarung ersetzt oder überarbeitet wird;

h. die Fähigkeit zur Übertragung der vorgesehenen Auslagerungsvereinbarung auf einen anderen Dienstleister, sofern dies notwendig oder wünschenswert ist, und zwar sowohl in vertraglicher als auch in praktischer Hinsicht, einschließlich der damit verbundenen geschätzten Risiken, der Hindernisse für die Geschäftsfortführung, der Kosten und des Zeitrahmens („Ersetzbarkeit“);

i. die Fähigkeit zur Wiedereingliederung der ausgelagerten Funktion in das Institut oder das Zahlungsinstitut, sofern dies notwendig oder wünschenswert ist;

j. den Schutz der Daten und die möglichen Folgen einer Verletzung der Vertraulichkeitspflichten oder des Versäumnisses, die Datenverfügbarkeit und -integrität sicherzustellen, sowohl für das Institut oder Zahlungsinstitut als auch für seine Kunden, unter anderem hinsichtlich der Einhaltung der Verordnung (EU) 2016/679[21].

[21] 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).

Titel III – Rahmen für die Governance

5 Solide Governance-Regelungen und Risiko durch Dritte („Third-Party Risk“)

32. Als Teil des gesamten internen Kontrollrahmenwerks, [22] einschließlich interner Kontrollmechanismen, [23] sollten die Institute und Zahlungsinstitute über ein ganzheitliches institutsweites Rahmenwerk für das Risikomanagement verfügen, das sich auf alle Geschäftsbereiche und internen Einheiten erstreckt. Gemäß diesem Rahmenwerk sollten die Institute und Zahlungsinstitute sämtliche ihrer Risiken, darunter auch Risiken, die durch Vereinbarungen mit Dritten verursacht werden, ermitteln und steuern. Das Rahmenwerk für das Risikomanagement sollte es den Instituten und Zahlungsinstituten ermöglichen, fundierte Entscheidungen zur Übernahme von Risiken zu treffen sowie die ordnungsgemäße Umsetzung von Risikomanagementmaßnahmen, auch mit Blick auf Cyberrisiken, sicherzustellen.[24]

33. Die Institute und Zahlungsinstitute sollten unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit in Einklang mit Abschnitt 1 alle auf Vereinbarungen mit Dritten zurückzuführenden Risiken, denen sie ausgesetzt sind oder ausgesetzt sein könnten, ermitteln, bewerten, überwachen und steuern, und zwar unabhängig davon, ob es sich bei diesen Vereinbarungen um Auslagerungsvereinbarungen handelt oder nicht. Die Risiken, insbesondere die operationellen Risiken, aller Vereinbarungen mit Dritten, einschließlich der in den Absätzen 26 und 28 Genannten, sollten in Einklang mit Abschnitt 12.2. bewertet werden.

34. Die Institute und Zahlungsinstitute sollten sicherstellen, dass sie alle Anforderungen gemäß der Verordnung (EU) 2016/679, auch was Vereinbarungen mit Dritten und Auslagerungsvereinbarungen betrifft, erfüllen.

6 Solide Governance-Regelungen und Auslagerungen

35. Die Auslagerung von Funktionen darf nicht zur Delegation der Verantwortlichkeiten des Leitungsorgans führen. Die Institute und Zahlungsinstitute bleiben in vollem Maße für die Erfüllung ihrer regulatorischen Pflichten verantwortlich und rechenschaftspflichtig, einschließlich der Fähigkeit zur Beaufsichtigung der Auslagerung von kritischen oder wesentlichen Funktionen.

36. Das Leitungsorgan ist stets mindestens für Folgendes in vollem Umfang verantwortlich und rechenschaftspflichtig:

---

[22] Die Institute sollten Titel V der EBA-Leitlinien zur internen Governance beachten.

[23] Siehe auch Artikel 11 der Richtlinie 2015/2366 (PSD2).

[24] Siehe auch EBA-Leitlinien zu Informations- und Kommunikationstechnologie (IT) und Sicherheitsrisikomanagement (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) und die grundlegenden Elemente der G7-Expertengruppe für das Management von Cyberrisiken durch Dritte im Finanzsektor (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

a. Sicherstellung, dass das Institut oder Zahlungsinstitut jederzeit die Bedingungen erfüllt, die zu erfüllen sind, um seine Zulassung zu behalten, einschließlich jeglicher von der zuständigen Behörde auferlegten Bedingungen;

b. die interne Organisation des Instituts oder des Zahlungsinstituts;

c. die Ermittlung, Bewertung und der Umgang mit Interessenkonflikten;

d. die Festlegung der Strategien und Richtlinien des Instituts oder Zahlungsinstituts (z. B. das Geschäftsmodell, die Risikobereitschaft, der Rahmen für das Risikomanagement);

e. die Beaufsichtigung des Tagesgeschäfts des Instituts oder Zahlungsinstituts, einschließlich der Steuerung aller mit einer Auslagerung verbundenen Risiken; sowie

f. die Überwachungsaufgabe des Leitungsorgans in seiner Aufsichtsfunktion, einschließlich der Beaufsichtigung und Überwachung der Entscheidungsprozesse der Geschäftsleitung.

37. Durch die Auslagerung dürfen die für die Mitglieder des Leitungsorgans des Instituts, der Direktoren oder der für das Management des Zahlungsinstituts bzw. Schlüsselfunktionsträger anzuwendenden Eignungskriterien nicht abgesenkt werden. Die Institute und Zahlungsinstitute sollten über eine angemessene Kompetenz sowie ausreichende und angemessen qualifizierte Ressourcen verfügen, um ein angemessenes Management und die Überwachung von Auslagerungsvereinbarungen sicherzustellen.

38. Die Institute und Zahlungsinstitute sollten

a. eine eindeutige Zuweisung der Zuständigkeiten für die Dokumentation, das Management und die Kontrolle von Auslagerungsvereinbarungen vornehmen;

b. ausreichende Mittel zuweisen, um die Erfüllung aller rechtlichen und aufsichtlichen Anforderungen zu gewährleisten, einschließlich der vorliegenden Leitlinien und der Dokumentation und Überwachung aller Auslagerungsvereinbarungen;

c. unter Berücksichtigung von Abschnitt 1 dieser Leitlinien eine Auslagerungsfunktion einrichten oder eine Führungskraft benennen, die unmittelbar dem Leitungsorgan unterstellt ist (z. B. ein Inhaber einer Schlüsselfunktion hinsichtlich einer Kontrollfunktion) und für die Steuerung und die Kontrolle der Risiken von Auslagerungsvereinbarungen als Teil des internen Kontrollrahmens des Instituts und die Überwachung der Dokumentation von Auslagerungsvereinbarungen verantwortlich ist. Kleine und weniger komplexe Institute oder Zahlungsinstitute sollten mindestens eine klare Trennung von Aufgaben und Zuständigkeiten für das Management und die Kontrolle von Auslagerungsvereinbarungen sicherstellen und können die Auslagerungsfunktion einem Mitglied des Leitungsorgans des Instituts oder Zahlungsinstituts übertragen.

39. Die Institute und Zahlungsinstitute sollten stets eine ausreichende Substanz wahren und nicht zu „leeren Hüllen“ oder „Briefkastenfirmen“ werden. Zu diesem Zweck sollten sie

    a. stets alle Voraussetzungen ihrer Zulassung[25] erfüllen, einschließlich der wirksamen Wahrnehmung seiner Zuständigkeiten durch das Leitungsorgan entsprechend den Ausführungen in Abschnitt 36 dieser Leitlinien;

    b. einen klaren und transparenten organisatorischen Rahmen und eine Struktur aufrechterhalten, die es ihnen ermöglichen, die Einhaltung der rechtlichen und aufsichtlichen Anforderungen sicherzustellen;

    c. bei der Auslagerung von operationellen Aufgaben von internen Kontrollfunktionen (z. B. im Fall einer gruppeninternen Auslagerung oder der Auslagerung im Rahmen von institutsbezogenen Sicherungssystemen) eine geeignete Aufsicht ausüben und die Fähigkeit zur Steuerung der Risiken besitzen, die durch die Auslagerung kritischer oder wesentlicher Funktionen entstehen; sowie

    d. über ausreichende Mittel und Kapazitäten verfügen, um die Erfüllung der Buchstaben a bis c sicherstellen.

40. Bei Auslagerungen sollten die Institute und Zahlungsinstitute mindestens sicherstellen, dass

    a. sie Entscheidungen bezüglich ihrer Geschäftstätigkeiten und kritischen oder wesentlichen Funktionen treffen und umsetzen können, einschließlich derjenigen, die Gegenstand einer Auslagerung sind;

    b. die Ordnungsmäßigkeit ihrer Geschäftstätigkeit und der erbrachten Bank- und Zahlungsdienste aufrechterhalten;

    c. die mit bestehenden oder geplanten Auslagerungsvereinbarungen verbundenen Risiken ordnungsgemäß ermittelt, bewertet, gesteuert und gemindert werden, einschließlich der mit der IT und Finanztechnologie verbundenen Risiken;

    d. geeignete Vertraulichkeitsvereinbarungen bezüglich der Daten und sonstigen Informationen bestehen;

[25] Siehe auch die technischen Regulierungsstandards gemäß Artikel 8 Absatz 2 der Richtlinie 2013/36/EU über die für die Zulassung von Kreditinstituten zu übermittelnden Informationen und die technischen Durchführungsstandards gemäß Artikel 8 Absatz 3 der Richtlinie 2013/36/EU für Standardformulare, Mustertexte und Verfahren zur Bereitstellung der Informationen, die für die Zulassung von Kreditinstituten erforderlich sind (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Für Zahlungsinstitute siehe die Leitlinien der EBA gemäß der Richtlinie (EU) 2015/2366 (PSD2) zu den Informationen, die für die Zulassung von Zahlungsinstituten und E-Geld-Instituten sowie für die Eintragung von Kontoinformationsdienstleistern zu übermitteln sind (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

e. ein angemessener Fluss an bedeutenden Informationen mit dem Dienstleister aufrechterhalten wird;

f. sie mit Blick auf die Auslagerung von kritischen oder wesentlichen Funktionen in der Lage sind, mindestens eine der folgenden Maßnahmen innerhalb eines angemessenen Zeitrahmens zu ergreifen:

   i. Übertragung der Funktion an alternative Dienstleister;

   ii. Wiedereingliederung der Funktion oder

   iii. Einstellung der von der Funktion abhängigen Geschäftstätigkeiten;

g. bei der Verarbeitung von personenbezogenen Daten durch einen Dienstleister in der EU und/oder in einem Drittland geeignete Maßnahmen durchgeführt werden und die Daten gemäß der Verordnung (EU) 2016/679 verarbeitet werden.

7 Auslagerungsrichtlinien

41. Das Leitungsorgan eines Instituts oder Zahlungsinstituts[26], das Auslagerungsvereinbarungen geschlossen hat oder den Abschluss solcher Vereinbarungen plant, sollte schriftliche Auslagerungsrichtlinien genehmigen, diese regelmäßig überprüfen und aktualisieren sowie deren Umsetzung auf individueller, teilkonsolidierter oder konsolidierter Basis sicherstellen. Für Institute sollten die Auslagerungsrichtlinien in Einklang mit Abschnitt 8 der Leitlinien der EBA zur internen Governance stehen und insbesondere sollten sie die in Abschnitt 18 (Neue Produkte und wesentliche Änderungen) dieser Leitlinien festgelegten Anforderungen berücksichtigen. Die Zahlungsinstitute können zudem ihre Richtlinien mit den Abschnitten 8 und 18 der Leitlinien der EBA zur internen Governance abstimmen.

42. Die Richtlinien sollten die zentralen Phasen des Lebenszyklus von Auslagerungsvereinbarungen umfassen und Definitionen der Grundsätze, Zuständigkeiten und Prozesse bezüglich Auslagerungen enthalten. Insbesondere sollten die Richtlinien mindestens folgende Gesichtspunkte abdecken:

   a. die Zuständigkeiten des Leitungsorgans in Einklang mit Absatz 36, gegebenenfalls einschließlich seiner Beteiligung an der Entscheidungsfindung zur Auslagerung kritischer oder wesentlicher Funktionen;

   b. die Einbindung der Geschäftsbereiche, der internen Kontrollfunktionen und sonstiger Personen in Auslagerungsvereinbarungen;

[26] Siehe auch die Leitlinien der EBA für Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der PSD2, abrufbar unter: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

c. die Planung von Auslagerungsvereinbarungen, einschließlich

   i. der Definition von Geschäftsanforderungen bezüglich Auslagerungsvereinbarungen;

   ii. der Kriterien, einschließlich derjenigen gemäß Abschnitt 4, und der Prozesse für die Ermittlung kritischer oder wesentlicher Funktionen;

   iii. der Ermittlung, Bewertung und Steuerung von Risiken gemäß Abschnitt 12.2;

   iv. einer Due-Diligence-Prüfung von künftigen Dienstleistern, einschließlich der nach Abschnitt 12.3 erforderlichen Maßnahmen;

   v. der Verfahren zur Ermittlung, Bewertung, Steuerung und Minderung potenzieller Interessenkonflikte gemäß Abschnitt 8;

   vi. der Planung der Geschäftsfortführung gemäß Abschnitt 9;

   vii. des Genehmigungsprozesses für neue Auslagerungsvereinbarungen;

d. die Umsetzung, Überwachung und das Management von Auslagerungsvereinbarungen, einschließlich

   i. der laufenden Bewertung der Leistung des Dienstleisters in Einklang mit Abschnitt 14;

   ii. der Verfahren für die Benachrichtigung über und die Reaktion auf Änderungen einer Auslagerungsvereinbarung oder bezüglich eines Dienstleisters (z. B. seiner Finanzlage, Organisations- oder Eigentumsstrukturen, Weiterverlagerungen);

   iii. der unabhängigen Prüfung der Erfüllung der rechtlichen und aufsichtlichen Anforderungen und Richtlinien;

   iv. der Verlängerungsverfahren;

e. die Dokumentation und Führung von Aufzeichnungen unter Berücksichtigung der Anforderungen in Abschnitt 11;

f. die Ausstiegsstrategien und Kündigungsverfahren, einschließlich der Anforderung eines dokumentierten Ausstiegsplans für jede auszulagernde kritische oder wesentliche Funktion, wenn ein solcher Ausstieg unter Berücksichtigung möglicher Dienstleistungsunterbrechungen oder einer unerwarteten Beendigung einer Auslagerungsvereinbarung für möglich erachtet wird.

43. Bei den Auslagerungsrichtlinien sollte zwischen Folgendem unterschieden werden:

a. Auslagerung kritischer oder wesentlicher Funktionen und sonstigen Auslagerungsvereinbarungen;

b. Auslagerung an Dienstleister, die von einer zuständigen Behörde zugelassen sind bzw. bei denen dies nicht der Fall ist;

c. gruppeninternen Auslagerungsvereinbarungen, Auslagerungsvereinbarungen innerhalb desselben institutsbezogenen Sicherungssystems (einschließlich Einrichtungen, die sich individuell oder kollektiv im Eigentum von Instituten innerhalb desselben institutsbezogenen Sicherungssystems befinden) und Auslagerungen an Einrichtungen außerhalb der Gruppe; sowie

d. Auslagerung an Dienstleister mit Sitz in einem Mitgliedstaat oder in Drittstaaten.

44. Die Institute und Zahlungsinstitute sollten sicherstellen, dass die Richtlinien die Ermittlung der folgenden potenziellen Auswirkungen von kritischen oder wesentlichen Auslagerungsvereinbarungen abdecken und dass diese beim Entscheidungsprozess berücksichtigt werden:

a. das Risikoprofil des Instituts;

b. die Fähigkeit, den Dienstleister zu überwachen und die Risiken zu steuern;

c. die Maßnahmen zur Geschäftsfortführung und

d. die Ausübung ihrer Geschäftstätigkeit.

8 Interessenkonflikte

45. In Einklang mit Titel IV Abschnitt 11 der Leitlinien der EBA zur internen Governance[27] sollten die Institute und Zahlungsinstitute Interessenkonflikte hinsichtlich ihrer Auslagerungsvereinbarungen erkennen, bewerten und regeln.

46. Wenn eine Auslagerung zu wesentlichen Interessenkonflikten führt, auch zwischen Einheiten innerhalb derselben Gruppe oder desselben institutsbezogenen Sicherungssystems, müssen die Institute und Zahlungsinstitute geeignete Maßnahmen ergreifen, um diese Interessenkonflikte zu regeln.

47. Wenn Funktionen durch einen Dienstleister erbracht werden, der Teil einer Gruppe oder Mitglied eines institutsbezogenen Sicherungssystems ist oder sich im Eigentum des Instituts, Zahlungsinstituts, der Gruppe oder von Instituten, die Mitglieder eines institutsbezogenen Sicherungssystems sind, befindet, sollten die Bedingungen, einschließlich der finanziellen Bedingungen, für die ausgelagerte Dienstleistung wie zwischen voneinander unabhängigen Geschäftspartnern festgelegt werden. Im Rahmen der Preisgestaltung der Dienstleistungen

[27] Zahlungsinstitute können ihre Richtlinien auch mit diesen Leitlinien abstimmen.

können jedoch Synergien, die durch die gleichen oder ähnliche Dienstleistungen für mehrere Institute innerhalb einer Gruppe oder eines institutsbezogenen Sicherungssystems entstehen, berücksichtigt werden, sofern der Dienstleister auf eigenständiger Basis tragfähig bleibt; innerhalb einer Gruppe sollte dies unabhängig vom Ausfall eines anderen Unternehmens dieser Gruppe sichergestellt sein.

9 Geschäftsfortführungspläne

48. In Einklang mit den Anforderungen nach Artikel 85 Absatz 2 der Richtlinie 2013/36/EU und Titel VI der Leitlinien der EBA zur internen Governance[28] sollten Institute und Zahlungsinstitute geeignete Geschäftsfortführungspläne hinsichtlich ausgelagerter kritischer oder wesentlicher Funktionen erstellen, diese pflegen und regelmäßig testen. Die Institute und Zahlungsinstitute innerhalb einer Gruppe oder eines institutsbezogenen Sicherungssystems können sich auf zentral festgelegte Geschäftsfortführungspläne hinsichtlich ihrer ausgelagerten Funktionen stützen.

49. Bei den Plänen zur Geschäftsfortführung sollte der mögliche Umstand berücksichtigt werden, dass sich die Qualität der Erbringung der ausgelagerten kritischen oder wesentlichen Funktion auf ein inakzeptables Niveau verschlechtert oder ihre Erbringung unterlassen wird. Bei solchen Plänen sind auch die möglichen Auswirkungen der Insolvenz oder eines anderen Ausfalls von Dienstleistern sowie gegebenenfalls politische Risiken in der Rechtsordnung des Dienstleisters zu berücksichtigen.

[28] Abrufbar unter: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

10 Funktion der Internen Revision

50. Die Tätigkeiten der Funktion der Internen Revision[29] sollten nach einem risikobasierten Ansatz die unabhängige Prüfung von ausgelagerten Tätigkeiten umfassen. Der Prüfplan[30] und das Prüfprogramm sollten insbesondere die Auslagerungsvereinbarungen für kritische oder wesentliche Funktionen umfassen.

51. Mit Blick auf den Auslagerungsprozess sollte die Funktion der internen Revision mindestens Folgendes überprüfen:

    a. die korrekte und wirksame Umsetzung des Rahmenwerks für Auslagerungen des Instituts oder Zahlungsinstituts, einschließlich der Auslagerungsrichtlinien, im Einklang mit den geltenden Gesetzen und Rechtsvorschriften, der Risikostrategie und den Entscheidungen des Leitungsorgans;

    b. die Angemessenheit, Qualität und Wirksamkeit der Bewertung der Kritikalität oder Wesentlichkeit von Funktionen;

    c. die Angemessenheit, Qualität und Wirksamkeit der Risikobewertung der Auslagerungsvereinbarungen sowie die Sicherstellung, dass die Risiken weiterhin mit der Risikostrategie des Instituts in Einklang stehen;

    d. die angemessene Einbindung von Leitungsorganen und

    e. die angemessene Überwachung und das Management von Auslagerungsvereinbarungen.

11 Dokumentationsanforderungen

52. Als Teil ihres Rahmenwerks für das Risikomanagement sollten die Institute und Zahlungsinstitute ein aktualisiertes Register mit Informationen über alle Auslagerungsvereinbarungen auf Institutsebene sowie gegebenenfalls auf teilkonsolidierter und konsolidierter Basis entsprechend den Ausführungen in Abschnitt 2 unterhalten und sollten alle bestehenden Auslagerungsvereinbarungen angemessen dokumentieren, wobei zwischen der Auslagerung kritischer oder wesentlicher Funktionen und sonstigen Auslagerungsvereinbarungen zu unterscheiden ist. Unter Berücksichtigung des nationalen

[29] Betreffend die Verantwortlichkeiten der Funktion der Internen Revision sollten die Institute auf Abschnitt 22 der Leitlinien der EBA zur internen Governance (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) und Zahlungsinstitute auf die Leitlinie 5 der Leitlinien der EBA zur Zulassung von Zahlungsinstituten (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf) Bezug nehmen.

[30] Siehe auch die Leitlinien der EBA zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs-und Bewertungsprozess (SREP): https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

Rechts sollten die Institute die Dokumentation von beendeten Auslagerungsvereinbarungen und die Begleitdokumentation für einen angemessenen Zeitraum weiterhin im Register führen.

53. Unter Berücksichtigung von Titel I der vorliegenden Leitlinien und unter den in Absatz 23 Buchstabe d festgelegten Bedingungen kann für die Institute und Zahlungsinstitute innerhalb einer Gruppe, die Institute, die ständig einer Zentralorganisation zugeordnet sind, bzw. die Institute, die Mitglieder desselben institutsbezogenen Sicherungssystems sind, das Register zentral geführt werden.

54. Das Register sollte mindestens die folgenden Informationen für alle bestehenden Auslagerungsvereinbarungen enthalten:

    a. eine Referenznummer für jede Auslagerungsvereinbarung;

    b. das Datum des Beginns und gegebenenfalls das Datum der nächsten Vertragsverlängerung, das Datum des Endes und/oder Kündigungsfristen für den Dienstleister und für das Institut oder Zahlungsinstitut;

    c. eine kurze Beschreibung der ausgelagerten Funktion, einschließlich der ausgelagerten Daten, sowie Angabe, ob personenbezogene Daten (z. B. durch Angabe von Ja oder Nein in einem gesonderten Datenfeld) übertragen werden oder ob ihre Verarbeitung an einen Dienstleister ausgelagert wird;

    d. eine vom Institut oder Zahlungsinstitut zugewiesene Kategorie, die die Art der Funktion entsprechend der Beschreibung unter Buchstabe c widerspiegelt (z. B. Informationstechnologie (IT), Kontrollfunktion) und die die Ermittlung verschiedener Arten von Vereinbarungen ermöglicht;

    e. den Namen des Dienstleisters, die Handelsregisternummer des Unternehmens, (sofern verfügbar) die Rechtsträgerkennung (LEI), die eingetragene Adresse und sonstige einschlägige Kontaktangaben sowie (gegebenenfalls) der Name des Mutterunternehmens;

    f. das Land bzw. die Länder, in dem/denen der Dienst erbracht werden soll, einschließlich des Standortes (d. h. Land oder Region), an dem sich die Daten befinden;

    g. die Angabe, ob die ausgelagerte Funktion als kritisch oder wesentliche eingestuft wird (Ja/Nein), gegebenenfalls einschließlich einer kurzen Zusammenfassung der Gründe, aus denen die ausgelagerte Funktion als kritisch oder wesentliche betrachtet wird;

    h. bei der Auslagerung zu einem Cloud-Anbieter das Cloud-Dienstmodell und das Cloud-Bereitstellungsmodell, d. h. öffentliche/private/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;

i. das Datum der letzten Bewertung der Kritikalität oder Wesentlichkeit der ausgelagerten Funktion.

55. Bei der Auslagerung von kritischen oder wesentlichen Funktionen sollte das Register mindestens die folgenden zusätzlichen Informationen enthalten:

a. die Institute, Zahlungsinstitute und sonstigen Unternehmen im aufsichtlichen Konsolidierungskreis bzw. Anwendungsbereich des institutsbezogenen Sicherungssystems, die von der Auslagerung Gebrauch machen;

b. die Angabe, ob der Dienstleister oder ein Subdienstleister Teil der Gruppe oder Mitglied des institutsbezogenen Sicherungssystems ist oder sich im Eigentum von Instituten oder Zahlungsinstituten innerhalb der Gruppe bzw. von Mitgliedern eines institutsbezogenen Sicherungssystems befindet oder nicht;

c. das Datum der letzten Risikobewertung und eine kurze Zusammenfassung der wesentlichsten Ergebnisse;

d. die Person oder das Entscheidungsgremium (z. B. das Leitungsorgan) in dem Institut oder Zahlungsinstitut, die bzw. das die Auslagerungsvereinbarung genehmigt hat;

e. das für die Auslagerungsvereinbarung geltende Recht;

f. gegebenenfalls das Datum der letzten und der nächsten geplanten Prüfung;

g. gegebenenfalls die Namen von Subunternehmern, an die wesentliche Teile einer kritischen oder wesentlichen Funktion weiter ausgelagert werden, einschließlich des Landes, in dem die Subunternehmer registriert sind, des Orts, an dem die Dienstleistung erbracht wird und gegebenenfalls des Orts (d. h. Land oder Region), an dem die Daten gespeichert werden;

h. das Ergebnis der Bewertung der Ersetzbarkeit des Dienstleisters (leicht, schwierig oder unmöglich), der Möglichkeit einer Wiedereingliederung einer kritischen oder wesentlichen Funktion in das Institut oder Zahlungsinstitut oder der Auswirkungen einer Einstellung der kritischen oder wesentlichen Funktion;

i. die Feststellung von alternativen Dienstleistern gemäß Buchstabe h;

j. die Angabe, ob die ausgelagerte kritische oder wesentliche Funktion Geschäftsvorgänge unterstützt, die zeitkritisch sind;

k. das veranschlagte jährliche Budget bzw. Kosten.

56. Die Institute und Zahlungsinstitute sollen auf Aufforderung der zuständigen Behörde entweder das vollständige Register aller bestehenden Auslagerungsvereinbarungen[31] oder bestimmte Teile desselben zur Verfügung stellen, wie etwa Informationen über alle Auslagerungsvereinbarungen, die unter eine der in Absatz 54 Buchstabe d dieser Leitlinien genannten Kategorien fallen (z. B. alle IT-Auslagerungsvereinbarungen). Die Institute und Zahlungsinstitute sollten diese Informationen in einem verarbeitbaren elektronischen Format bereitstellen (z. B. ein allgemein verwendetes Datenbankformat oder im CSV-Format (Comma Separated Values)).

57. Die Institute und Zahlungsinstitute sollten auf Aufforderung der zuständigen Behörde alle Informationen zur Verfügung stellen, die notwendig sind, damit die zuständige Behörde die wirksame Beaufsichtigung des Instituts oder des Zahlungsinstituts durchführen kann, gegebenenfalls einschließlich einer Kopie der Auslagerungsvereinbarung.

58. Unbeschadet von Artikel 19 Absatz 6 der Richtlinie (EU) 2015/2366 sollten die Institute und Zahlungsinstitute die zuständigen Behörden rechtzeitig über die geplante Auslagerung von kritischen oder wesentlichen Funktionen informieren oder in einen aufsichtlichen Dialog mit den zuständigen Behörden treten und/oder mindestens die in Absatz 54 aufgeführten Informationen bereitstellen, wenn eine ausgelagerte Funktion kritisch oder wesentlich geworden ist.

59. Die Institute und Zahlungsinstitute[32] sollten die zuständigen Behörden rechtzeitig über wesentliche Änderungen und/oder schwerwiegende Vorfälle bezüglich ihrer Auslagerungsvereinbarungen, die wesentliche Auswirkungen auf die Fortführung von Geschäftstätigkeiten der Institute oder Zahlungsinstitute aufweisen können, in Kenntnis setzen.

60. Die Institute und Zahlungsinstitute sollten die gemäß Titel IV vorgenommenen Bewertungen und die Ergebnisse ihrer fortlaufenden Überwachung (z. B. Leistung des Dienstleisters, Erfüllung einer vereinbarten Dienstleistungsgüte, sonstige vertragliche und aufsichtliche Anforderungen, Aktualisierungen der Risikobewertung) angemessen dokumentieren.

Titel IV – Auslagerungsprozess

12 Analyse vor der Auslagerung

61. Vor dem Abschluss einer Auslagerungsvereinbarung sollten die Institute und Zahlungsinstitute

    a. bewerten, ob die Auslagerungsvereinbarung gemäß den Ausführungen in Titel II eine kritische oder wesentliche Funktion betrifft,

[31] Siehe auch die Leitlinien der EBA zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs-und Bewertungsprozess (SREP), abrufbar unter: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[32] Siehe auch die Leitlinien der EBA für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD2), abrufbar unter: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

b. bewerten, ob die aufsichtlichen Bedingungen für eine Auslagerung gemäß Abschnitt 12.1 erfüllt sind;

c. alle einschlägigen Risiken der Auslagerungsvereinbarung gemäß Abschnitt 12.2 ermitteln und bewerten;

d. eine angemessene Due-Diligence-Prüfung des künftigen Dienstleisters gemäß Abschnitt 12.3 vornehmen;

e. gemäß Abschnitt 8 Interessenkonflikte, die durch die Auslagerung entstehen können, erkennen und bewerten.

12.1 Aufsichtliche Bedingungen für eine Auslagerung

62. Die Institute und Zahlungsinstitute sollten sicherstellen, dass die Auslagerung von Funktionen des Bankgeschäfts[33] oder der Zahlungsdienste in einem Umfang, in dem für die Wahrnehmung der betreffenden Funktion eine Zulassung oder Registrierung durch eine zuständige Behörde in dem Mitgliedstaat ihrer Zulassung erforderlich ist, an einen Dienstleister mit Sitz im selben oder in einem anderen Mitgliedstaat nur erfolgt, wenn die folgenden Bedingungen erfüllt sind:

    a. der Dienstleister ist von einer zuständigen Behörde für die Erbringung solcher Bankgeschäfte oder Zahlungsdienste zugelassen oder registriert; oder

    b. dem Dienstleister ist es anderweitig gestattet, solche Bankgeschäfte oder Zahlungsdienste in Einklang mit dem einschlägigen nationalen Rechtsrahmen durchzuführen.

63. Die Institute und Zahlungsinstitute sollten sicherstellen, dass die Auslagerung von Funktionen des Bankgeschäfts oder der Zahlungsdienste in einem Umfang, in dem für die Wahrnehmung der betreffenden Funktion eine Zulassung oder Registrierung durch eine zuständige Behörde in dem Mitgliedstaat ihrer Zulassung erforderlich ist, an einen Dienstleister mit Sitz in einem Drittstaat nur erfolgt, wenn die folgenden Bedingungen erfüllt sind:

    a. Der Dienstleister ist in dem Drittstaat für die Erbringung solcher Bankgeschäfte oder Zahlungsdienste zugelassen oder registriert und wird von einer einschlägigen zuständigen Behörde in dem betreffenden Drittstaat beaufsichtigt („Aufsichtsbehörde“);

    b. es besteht eine entsprechende Kooperationsvereinbarung, z. B. in Form einer Absichtserklärung („Memorandum of Understanding“) oder College-Vereinbarung -, zwischen den für die Beaufsichtigung des Instituts zuständigen Behörden und den für die Beaufsichtigung des Dienstleisters zuständigen Aufsichtsbehörden; und

[33] Siehe Artikel 9 der CRD bezüglich des Verbots der Entgegennahme von Einlagen oder anderen rückzahlbaren Geldern des Publikums durch Personen oder Unternehmen, die keine Kreditinstitute sind.

c. die in Buchstabe b genannte Kooperationsvereinbarung sollte sicherstellen, dass die zuständigen Behörden mindestens in der Lage sind,

i. die für die Durchführung ihrer Aufsichtsfunktionen gemäß der Richtlinie 2013/36/EU, der Verordnung (EU) Nr. 575/2013, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG notwendigen Informationen auf Anfrage zu erhalten;

ii. angemessenen Zugang zu Daten, Dokumenten, Räumlichkeiten oder Personal in dem Drittstaat, die für die Durchführung ihrer Aufsichtsbefugnisse von Belang sind, zu erhalten;

iii. so bald wie möglich Informationen von der Aufsichtsbehörde in dem Drittstaat für die Untersuchung offensichtlicher Verstöße gegen die Anforderungen der Richtlinie 2013/36/EU, der Verordnung (EU) Nr. 575/2013, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG zu erhalten; und

iv. mit den einschlägigen Aufsichtsbehörden in dem Drittstaat bei der Durchsetzung im Fall eines Verstoßes gegen die geltenden aufsichtlichen Anforderungen und das nationale Recht des Mitgliedstaates zusammenzuarbeiten. Die Zusammenarbeit sollte den Erhalt von Informationen über mögliche Verstöße gegen geltende aufsichtliche Anforderungen von den Aufsichtsbehörden in dem Drittstaat, sobald sich dies praktisch durchführen lässt, umfassen, ist aber nicht zwangsläufig darauf beschränkt.

12.2 Risikobewertung von Auslagerungsvereinbarungen

64. Die Institute und Zahlungsinstitute sollten die möglichen Auswirkungen von Auslagerungsvereinbarungen auf ihr operationelles Risiko bewerten, sie sollten die Ergebnisse der Bewertung bei der Entscheidung berücksichtigen, ob die Funktion an einen Dienstleister ausgelagert werden sollte, und geeignete Schritte einleiten, um unnötige zusätzliche operationelle Risiken vor dem Abschluss von Auslagerungsvereinbarungen zu vermeiden.

65. Die Bewertung sollte gegebenenfalls Szenarien möglicher Risikoereignisse einschließen, darunter auch operationelle Risikoereignisse mit gravierenden Folgen. Im Rahmen der Szenarioanalyse sollten die Institute und Zahlungsinstitute die möglichen Auswirkungen von unterlassenen oder unzureichenden Dienstleistungen bewerten, darunter die Risiken, die durch Prozesse, Systeme, Menschen oder externe Ereignisse verursacht werden. Die Institute und Zahlungsinstitute sollten unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach Abschnitt 1 die vorgenommene Analyse und ihre Ergebnisse dokumentieren und sie sollten den Umfang schätzen, in dem ihr operationelles Risiko durch die Auslagerungsvereinbarung erhöht oder verringert wird. Unter Berücksichtigung von Titel I können kleine und nicht komplexe Institute und Zahlungsinstitute qualitative Ansätze für die

Risikobewertung heranziehen, während große oder komplexe Institute einen komplexeren Ansatz wählen sollten, sofern verfügbar, einschließlich der Verwendung interner und externer Verlustdaten als Grundlage für die Szenarioanalyse.

66. Im Rahmen der Risikobewertung sollten die Institute und Zahlungsinstitute auch die erwarteten Vorteile und Kosten der geplanten Auslagerungsvereinbarung berücksichtigen, einschließlich der Abwägung etwaiger Risiken, die verringert oder besser gesteuert werden können, gegenüber Risiken, die durch die geplante Auslagerungsvereinbarung entstehen können, wobei mindestens folgende Punkte zu berücksichtigen sind:

    a. Konzentrationsrisiken, unter anderem durch

        i. die Auslagerung an einen beherrschenden Dienstleister, der nicht leicht zu ersetzen ist; und

        ii. mehrere Auslagerungsvereinbarungen mit demselben Dienstleister oder eng miteinander verbundenen Dienstleistern;

    b. die aggregierten Risiken, die auf die Auslagerung mehrerer Funktionen im gesamten Institut oder Zahlungsinstitut zurückgehen, sowie im Fall von Gruppen von Instituten oder institutsbezogenen Sicherungssystemen die aggregierten Risiken auf konsolidierter Basis oder Basis des institutsbezogenen Sicherungssystems;

    c. im Fall von bedeutenden Instituten das „Step-in risk“, d. h. das Risiko, das durch die erforderliche Bereitstellung finanzieller Unterstützung für einen Dienstleister in einer Notsituation oder die Übernahme seiner Geschäftstätigkeit entstehen kann; und

    d. die von dem Institut oder Zahlungsinstitut sowie dem Dienstleister ergriffenen Maßnahmen zur Steuerung und Minderung der Risiken.

67. Wenn die Auslagerungsvereinbarung die Möglichkeit beinhaltet, dass der Dienstleister kritische oder wesentliche Funktionen an andere Dienstleister weiterverlagert, sollten die Institute und Zahlungsinstitute Folgendes berücksichtigen:

    a. die mit der Weiterverlagerung verbundenen Risiken, darunter die zusätzlichen Risiken, die entstehen können, wenn der Subunternehmer seinen Sitz in einem Drittstaat oder einem anderen Land als der Dienstleister hat;

    b. das Risiko, dass durch lange und komplexe Auslagerungsketten die Fähigkeit der Institute oder Zahlungsinstitute zur Überwachung der ausgelagerten kritischen oder wesentlichen Funktion und die Fähigkeit der zuständigen Behörden zu einer wirksamen Beaufsichtigung eingeschränkt werden.

68. Bei der Durchführung der Risikobewertung vor der Auslagerung und während der laufenden Überwachung der Leistung des Dienstleisters sollten die Institute und Zahlungsinstitute mindestens

a. die einschlägigen Funktionen und entsprechenden Daten und Systeme hinsichtlich ihrer Sensitivität und der erforderlichen Sicherheitsmaßnahmen ermitteln und einstufen;

b. eine gründliche risikobasierte Analyse der Funktionen und entsprechenden Daten und Systeme durchführen, die für eine Auslagerung infrage kommen oder ausgelagert wurden, sowie den potenziellen Risiken Rechnung tragen, insbesondere den operationellen Risiken, einschließlich der rechtlichen Risiken, IT-, Compliance- und Reputationsrisiken, sowie Einschränkungen bei der Beaufsichtigung in Ländern, in denen die ausgelagerten Dienstleistungen erbracht werden oder erbracht werden können bzw. in denen die Daten gespeichert oder wahrscheinlich gespeichert werden, berücksichtigen;

c. die Folgen des Standortes der Niederlassung des Dienstleisters (innerhalb oder außerhalb der EU) berücksichtigen;

d. die politische Stabilität und Sicherheitslage der betreffenden Rechtsordnungen berücksichtigen, einschließlich

   i. der geltenden Gesetze, darunter auch die Gesetze zum Datenschutz;

   ii. der geltenden Vorschriften zur Rechtsdurchsetzung; und

   iii. der insolvenzrechtlichen Vorschriften, die bei einem Ausfall des Dienstleisters Anwendung fänden, sowie etwaiger Einschränkungen, die insbesondere bezüglich der dringenden Wiederherstellung der Daten des Instituts oder Zahlungsinstituts entstehen könnten;

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

f. Prüfung, ob der Dienstleister ein Tochterunternehmen oder Mutterunternehmen des Instituts ist, zum Konsolidierungskreis der Rechnungslegung zählt oder ein Mitglied bzw. im Eigentum von Instituten ist, die Mitglieder eines institutsbezogenen Sicherungssystems sind, sowie in diesem Fall Ermittlung des Umfangs, in dem das Institut diesen kontrolliert oder über Möglichkeiten zur Beeinflussung seiner Maßnahmen in Einklang mit Abschnitt 2 verfügt.

12.3 Due-Diligence-Prüfung

69. Vor dem Abschluss einer Auslagerungsvereinbarung und der Prüfung der operationellen Risiken in Zusammenhang mit der auszulagernden Funktion sollten die Institute und Zahlungsinstitute im Rahmen ihres Auswahl- und Bewertungsverfahrens sicherstellen, dass der Dienstleister geeignet ist.

70. Was kritische oder wesentliche Funktionen betrifft, so sollten die Institute und Zahlungsinstitute sicherstellen, dass der Dienstleister über die geschäftliche Reputation, angemessene und ausreichende Fähigkeiten, Fachkenntnisse, Kapazitäten, Mittel (z. B. personelle und finanzielle Mittel, IT-Ressourcen), Organisationsstruktur und gegebenenfalls die erforderliche(n) aufsichtliche(n) Zulassung(en) oder Registrierung(en) zur Wahrnehmung der kritischen oder wesentlichen Funktion in zuverlässiger und professioneller Weise verfügt, um seine Verpflichtungen während der Laufzeit des Vertragsentwurfs zu erfüllen.

71. Zu den zusätzlichen Faktoren, die bei der Durchführung einer Sorgfaltsprüfung eines potenziellen Dienstleisters zu berücksichtigen sind, zählen Folgende:

    a. sein Geschäftsmodell, seine Art, sein Umfang, seine Komplexität, Finanzlage, Eigentums- und Gruppenstruktur;

    b. die langfristigen Beziehungen mit Dienstleistern, die bereits bewertet wurden, und Dienstleistungen für das Institut oder Zahlungsinstitut erbringen;

    c. der Umstand, ob der Dienstleister ein Mutterunternehmen oder Tochterunternehmen des Instituts oder Zahlungsinstituts ist, zum Konsolidierungskreis der Rechnungslegung des Instituts zählt oder Mitglied bzw. im Eigentum von Instituten ist, die Mitglieder desselben institutsbezogenen Sicherungssystems sind, zu dem das Institut gehört;

    d. der Umstand, ob der Dienstleister von zuständigen Behörden beaufsichtigt wird.

72. Wenn die Auslagerung die Verarbeitung personenbezogener oder vertraulicher Daten umfasst, sollten sich die Institute und Zahlungsinstitute davon überzeugen, dass der Dienstleister angemessene technische und organisatorische Maßnahmen zum Schutz der Daten umsetzt.

73. Die Institute und Zahlungsinstitute sollten geeignete Schritte unternehmen, um sicherzustellen, dass die Dienstleister in einer mit ihren Werten und ihrem Verhaltenskodex im Einklang stehender Weise handeln. Insbesondere mit Blick auf Dienstleister mit Sitz in Drittstaaten und gegebenenfalls ihre Subunternehmer sollten sich die Institute und Zahlungsinstitute davon überzeugen, dass der Dienstleister in einer ethisch und sozial verantwortlichen Weise handelt und die international anerkannten Normen zu den Menschenrechten (z. B. die Europäische Menschenrechtskonvention), zum Umweltschutz und zu angemessenen Arbeitsbedingungen, einschließlich des Verbots von Kinderarbeit, erfüllt.

13 Vertragsphase

74. Die Rechte und Pflichten des Instituts, des Zahlungsinstituts und des Dienstleisters sollten eindeutig festgelegt und in einer schriftlichen Vereinbarung festgehalten sein.

75. Die Auslagerungsvereinbarung für kritische oder wesentliche Funktionen sollte mindestens folgende Bestimmungen enthalten:

    a. eine klare Beschreibung der zu erbringenden ausgelagerten Funktion;

    b. das Datum des Beginns und gegebenenfalls des Endes der Vereinbarung sowie die Kündigungsfristen für den Dienstleister und das Institut oder Zahlungsinstitut;

    c. das für die Vereinbarung geltende Recht;

    d. die finanziellen Pflichten der Parteien;

    e. die Angabe, ob die Weiterverlagerung einer kritischen oder wesentlichen Funktion bzw. Teile derselben zulässig ist; ist dies der Fall, sind die in Abschnitt 13.1. aufgeführten Bedingungen für die Weiterverlagerung anzugeben;

    f. den Standort bzw. die Standorte (d. h. Regionen oder Länder), in denen die Durchführung einer kritischen oder wesentlichen Funktion erfolgt und/oder maßgebliche Daten gespeichert und verarbeitet werden, einschließlich des möglichen Speicherortes, und die zu erfüllenden Bedingungen, einschließlich der Anforderung, das Institut oder Zahlungsinstitut zu benachrichtigen, wenn der Dienstleister den Standort/die Standorte wechselt;

    g. gegebenenfalls Bestimmungen betreffend die Zugänglichkeit, Verfügbarkeit, Integrität, den Datenschutz und die Sicherheit der entsprechenden Daten gemäß Abschnitt 13.2;

    h. das Recht des Instituts oder Zahlungsinstituts auf laufende Überwachung der Leistung des Dienstleisters;

    i. die vereinbarte Dienstleistungsgüte, die genaue quantitative und qualitative Leistungsziele für die ausgelagerte Funktion umfassen sollte, um eine termingerechte Überwachung zu ermöglichen, sodass ohne größere Verzögerung eine geeignete Korrekturmaßnahme ergriffen werden kann, wenn die Dienstleistungsgüte nicht erfüllt wird;

    j. die Berichtspflichten des Dienstleisters gegenüber dem Institut oder Zahlungsinstitut, einschließlich der Übermittlung von Informationen durch den Dienstleister über Entwicklungen mit möglicherweise nachteiligen Auswirkungen auf die Fähigkeit des Dienstleisters zur wirksamen Durchführung der kritischen oder wesentlichen Funktion gemäß der vereinbarten Dienstleistungsgüte, den geltenden Gesetzen und aufsichtlichen Anforderungen, sowie gegebenenfalls die Pflichten zur Vorlage von Berichten der Funktion der inneren Revision des Dienstleisters;

    k. Angabe, ob der Dienstleister verpflichtet wird für bestimmte Risiken eine Versicherung abzuschließen, sowie gegebenenfalls die Höhe der geforderten Versicherungsdeckung;

l. die Anforderungen für die Umsetzung und Erprobung von Notfallplänen;

m. Bestimmungen, mit denen sichergestellt wird, dass auf die sich im Besitz des Instituts oder des Zahlungsinstituts befindlichen Daten im Fall einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des Dienstleisters zugegriffen werden kann;

n. die Pflicht des Dienstleisters zur Zusammenarbeit mit den zuständigen Behörden und Abwicklungsbehörden des Instituts oder Zahlungsinstituts, einschließlich weiterer von diesen ernannter Personen;

o. für Institute einen klaren Verweis auf die Befugnisse der nationalen Abwicklungsbehörde, insbesondere auf die Artikel 68 und 71 der Richtlinie 2014/59/EG (BRRD) und vor allem eine Beschreibung der „wesentlichen vertraglichen Verpflichtungen“ im Sinne von Artikel 68 dieser Richtlinie;

p. das uneingeschränkte Recht der Institute, Zahlungsinstitute und zuständigen Behörden zur Kontrolle und Prüfung des Dienstleisters, insbesondere was die ausgelagerte kritische oder wesentliche Funktion betrifft, gemäß den Ausführungen in Abschnitt 13.3;

q. Kündigungsrechte gemäß Abschnitt 13.4.

13.1 Weiterverlagerung von kritischen oder wesentlichen Funktionen

76. In der Auslagerungsvereinbarung sollte angegeben sein, ob die Weiterverlagerung von kritischen oder wesentlichen Funktionen bzw. von wesentlichen Teilen derselben zulässig ist oder nicht.

77. Sofern die Weiterverlagerung von kritischen oder wesentlichen Funktionen zulässig ist, sollten die Institute oder Zahlungsinstitute festlegen, ob der weiter zu verlagernde Teil der Funktion an sich kritisch oder wesentlich ist (d. h. einen wesentlichen Teil der kritischen oder wesentlichen Funktion darstellt), und diesen gegebenenfalls im Register erfassen.

78. Sofern die Weiterverlagerung von kritischen oder wesentlichen Funktionen zulässig ist, sollte in der schriftlichen Vereinbarung Folgendes festgehalten werden:

a. Angabe etwaiger Arten von Tätigkeiten, die von einer Weiterverlagerung ausgeschlossen sind;

b. Angabe der im Fall einer Weiterverlagerung zu erfüllenden Bedingungen;

c. Angabe, dass der Dienstleister verpflichtet ist, die von ihm weiterverlagerten Dienstleistungen zu überwachen, um sicherzustellen, dass alle vertraglichen Pflichten

zwischen dem Dienstleister und dem Institut oder Zahlungsinstitut fortlaufend erfüllt werden;

d. Verpflichtung des Dienstleisters, vor der Weiterverlagerung in Zusammenhang mit Daten vorab eine spezifische oder allgemeine schriftliche Genehmigung vom Institut oder Zahlungsinstitut einzuholen;[34]

e. Aufnahme einer Pflicht des Dienstleisters, das Institut oder Zahlungsinstitut über eine geplante Weiterverlagerung bzw. geplante wesentliche Änderungen derselben zu informieren, insbesondere wenn diese Auswirkungen auf die Fähigkeit des Dienstleisters zur Erfüllung seiner Pflichten gemäß der Auslagerungsvereinbarung haben könnte. Dies umfasst geplante wesentliche Änderungen hinsichtlich Subunternehmern und die Frist für Benachrichtigungen; insbesondere sollte es die festzusetzende Frist für Benachrichtigungen dem auslagernden Institut oder Zahlungsinstitut mindestens ermöglichen, eine Risikobewertung der geplanten Änderungen vorzunehmen und den Änderungen zu widersprechen, bevor die geplante Weiterverlagerung oder wesentliche Änderungen derselben in Kraft treten;

f. gegebenenfalls Sicherstellung, dass das Institut oder Zahlungsinstitut befugt ist, die beabsichtigte Weiterverlagerung oder wesentliche Änderung derselben abzulehnen, oder das Erfordernis einer expliziten Genehmigung;

g. Sicherstellung, dass das Institut oder Zahlungsinstitut über das vertragliche Recht zur Kündigung der Vereinbarung bei einer unzulässigen Weiterverlagerung verfügt, z. B. wenn sich durch die Weiterverlagerung die Risiken für das Institut oder Zahlungsinstitut wesentlich erhöhen oder der Dienstleister eine Weiterverlagerung vornimmt, ohne das Institut oder Zahlungsinstitut zu benachrichtigen.

79. Die Institute und Zahlungsinstitute sollten vereinbaren, dass eine Weiterverlagerung nur erfolgt, wenn sich der Subunternehmer dazu verpflichtet,

    a. alle geltenden Gesetze, aufsichtlichen Anforderungen und vertraglichen Pflichten zu erfüllen; und

    b. dem Institut, Zahlungsinstitut und der zuständigen Behörde dieselben vertraglichen Rechte auf Zugang und Prüfung einzuräumen, die vom Dienstleister gewährt werden.

80. Die Institute und Zahlungsinstitute sollten sicherstellen, dass der Dienstleister die Subunternehmer gemäß den von dem Institut oder Zahlungsinstitut festgelegten Richtlinien angemessen überwacht. Sofern die geplante Weiterverlagerung wesentliche nachteilige Auswirkungen auf die Auslagerungsvereinbarung über eine kritische oder wesentliche Funktion aufweisen könnte oder zu einem wesentlich höheren Risiko führen würde, auch wenn die Bedingungen in Absatz 79 nicht erfüllt sind, sollte das Institut oder Zahlungsinstitut sein Recht

[34] Siehe Artikel 28 der Verordnung (EU) 2016/679.

auf Ablehnung der Weiterverlagerung ausüben, wenn ein solches Recht vereinbart wurde, und/oder den Vertrag kündigen.

13.2 Sicherheit von Daten und Systemen

81. Die Institute und Zahlungsinstitute sollten sicherstellen, dass die Dienstleister sofern notwendig geeignete IT-Sicherheitsstandards erfüllen.

82. Sofern notwendig (z. B. im Rahmen von Cloud-Outsourcing oder sonstigen Auslagerungen im IT-Bereich), sollten die Institute und Zahlungsinstitute Anforderungen an die Daten- und Systemsicherheit im Rahmen der Auslagerungsvereinbarung festlegen und die Einhaltung dieser Anforderungen fortlaufend überwachen.

83. Bei einer Auslagerung an Cloud-Dienste und sonstigen Auslagerungsvereinbarungen, die den Umgang mit oder die Übertragung von personenbezogenen oder vertraulichen Daten umfassen, sollten die Institute und Zahlungsinstitute einen risikobasierten Ansatz betreffend den Standort bzw. die Standorte der Datenspeicherung und Datenverarbeitung (d. h. Land oder Region) und hinsichtlich Überlegungen zur Informationssicherheit wählen.

84. Unbeschadet der Anforderungen gemäß der Verordnung (EU) 2016/679 sollten die Institute und Zahlungsinstitute bei Auslagerungen (insbesondere in Drittstaaten) die Unterschiede bei den nationalen Vorschriften für den Datenschutz berücksichtigen. Die Institute und Zahlungsinstitute sollten sicherstellen, dass in der Auslagerungsvereinbarung die Pflicht des Dienstleisters festgelegt ist, vertrauliche, personenbezogene und anderweitig sensible Informationen zu schützen und alle rechtlichen Anforderungen den Datenschutz betreffend zu erfüllen, die für das Institut oder Zahlungsinstitut gelten (z. B. der Schutz von personenbezogenen Daten und die Einhaltung des Bankgeheimnisses oder vergleichbarer rechtlicher Geheimhaltungspflichten hinsichtlich der Informationen der Kunden).

13.3 Zugangs-, Informations- und Prüfungsrechte

85. Die Institute und Zahlungsinstitute sollten im Rahmen der schriftlichen Auslagerungsvereinbarung sicherstellen, dass die Funktion der Internen Revision in der Lage ist, die ausgelagerte Funktion unter Verwendung eines risikobasierten Ansatzes zu prüfen.

86. Unabhängig von der Kritikalität oder Wesentlichkeit der ausgelagerten Funktion sollte in den schriftlichen Auslagerungsvereinbarungen zwischen den Instituten und Dienstleistern auf die Informationserfassung und Untersuchungsbefugnisse der zuständigen Behörden und Abwicklungsbehörden gemäß Artikel 63 Absatz 1 Buchstabe a der Richtlinie 2014/59/EU und Artikel 65 Absatz 3 der Richtlinie 2013/36/EU mit Blick auf Dienstleister mit Sitz in einem Mitgliedstaat Bezug genommen werden und es sollten darüber hinaus diese Rechte bezüglich Dienstleistern mit Sitz in Drittstaaten gewährleistet werden.

87. Was die Auslagerung von kritischen oder wesentlichen Funktionen anbelangt, so sollten die Institute und Zahlungsinstitute im Rahmen der Auslagerungsvereinbarung sicherstellen, dass

der Dienstleister ihnen und ihren zuständigen Behörden, einschließlich der Abwicklungsbehörden, und jeder anderen von ihnen oder den zuständigen Behörden benannten Person Folgendes gewährt:

a. vollständigen Zugang zu allen relevanten Geschäftsräumen (z. B. Hauptsitze und Betriebszentren), einschließlich des gesamten Spektrums an relevanten Geräten, Systemen, Netzwerken, Informationen und Daten, die für die Wahrnehmung der ausgelagerten Funktion eingesetzt werden, auch in Zusammenhang mit Finanzinformationen, Personal und den externen Prüfern des Dienstleisters („Zugangs- und Informationsrechte“); sowie

b. uneingeschränkte Rechte auf Kontrolle und Prüfung in Zusammenhang mit der Auslagerungsvereinbarung („Prüfungsrechte“), um ihnen die Überwachung der Auslagerungsvereinbarung zu ermöglichen und die Einhaltung aller geltenden aufsichtlichen und vertraglichen Anforderungen sicherzustellen.

88. Für die Auslagerung von Funktionen, die nicht kritisch oder wesentlich sind, sollten die Institute und Zahlungsinstitute die Zugangs- und die Prüfungsrechte entsprechend den Ausführungen in Absatz 87 Buchstaben a und b und in Abschnitt 13.3 auf einem risikobasierten Ansatz sicherstellen, wobei die Art der ausgelagerten Funktion und die dazugehörigen operationellen Risiken und Reputationsrisiken, ihre Skalierbarkeit, die potenziellen Auswirkungen auf die kontinuierliche Ausübung der Tätigkeiten und die Vertragslaufzeit zu berücksichtigen sind. Die Institute und Zahlungsinstitute sollten berücksichtigen, dass Funktionen im Laufe der Zeit kritisch oder wesentlich werden können.

89. Die Institute und Zahlungsinstitute sollten sicherstellen, dass die Auslagerungsvereinbarung oder etwaige anderen vertraglichen Regelungen der wirksamen Ausübung der Zugangs- und Prüfungsrechte durch sie selbst, die zuständigen Behörden oder von ihnen für die Ausübung dieser Rechte ernannte Dritte nicht im Wege stehen oder diese einschränken.

90. Die Institute und Zahlungsinstitute sollten ihre Zugangs- und Prüfungsrechte ausüben, die Häufigkeit der Prüfungen und die zu prüfenden Bereiche nach einem risikobasierten Ansatz bestimmen und die maßgeblichen, allgemein akzeptierten nationalen und internationalen Prüfstandards einhalten.[35]

91. Unbeschadet ihrer letztendlichen Verantwortung für Auslagerungsvereinbarungen können Institute und Zahlungsinstitute Folgendes nutzen:

a. Sammelprüfungen („pooled audits“), die gemeinsam mit anderen Kunden desselben Dienstleisters organisiert und von ihnen und diesen Kunden oder einem von den Kunden beauftragten Dritten durchgeführt werden, sodass die Prüfungsressourcen

[35] Weiterführende Informationen für Institute finden sich in Abschnitt 22 der EBA-Leitlinien zur internen Governance: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

effizienter genutzt werden und der Organisationsaufwand für die Kunden und den Dienstleister verringert wird.

b. Zertifizierungen durch Dritte und externe oder interne Revisionsberichte, die vom Dienstleister zur Verfügung gestellt werden.

92. Für die Auslagerung von kritischen oder wesentlichen Funktionen sollten die Institute und Zahlungsinstitute bewerten, ob Zertifizierungen durch Dritte und Berichte entsprechend Absatz 91 Buchstabe b angemessen und hinreichend sind, um ihre aufsichtlichen Pflichten zu erfüllen, und sollten sich nicht dauerhaft ausschließlich auf diese Berichte verlassen.

93. Die Institute und Zahlungsinstitute sollten die in Absatz 91 Buchstabe b genannten Methoden nur verwenden, wenn sie

a. mit dem Prüfungsplan für die ausgelagerte Funktion zufrieden sind;

b. sicherstellen, dass sich der Zertifizierungs- oder Prüfberichtsumfang auf die Systeme (d. h. Prozesse, Anwendungen, Infrastruktur, Rechenzentren usw.) sowie die wichtigsten Kontrollen, die vom Institut oder Zahlungsinstitut ermittelt wurden, und die Einhaltung der maßgeblichen aufsichtlichen Anforderungen erstreckt;

c. laufend den Inhalt der Zertifizierungen und Prüfberichte sorgfältig bewerten und überprüfen, dass die Berichte oder Zertifizierungen nicht veraltet sind;

d. sicherstellen, dass die Schlüsselsysteme und Kontrollen in künftigen Versionen der Zertifizierung oder des Prüfberichts berücksichtigt werden;

e. mit der Eignung der Zertifizierers oder Prüfers zufrieden sind (beispielsweise hinsichtlich der Rotation des Zertifizierungs- oder Prüfungsunternehmens, der Qualifikationen, des Fachwissens oder der Neudurchführung/Überprüfung der Nachweise in der zugrunde liegenden Prüfdatei);

f. sich davon überzeugt haben, dass die Zertifizierungen und die Prüfungen auf der Grundlage allgemein anerkannter einschlägiger professioneller Standards erfolgen und einen Test der operativen Wirksamkeit der vorhandenen wichtigsten Kontrollen beinhalten;

g. über das vertragliche Recht verfügen, die Erweiterung des Umfangs der Zertifizierungen oder Prüfberichte auf weitere einschlägige Systeme und Kontrollen zu verlangen; die Zahl und Häufigkeit solcher Ersuchen um Änderungen des Umfangs sollten sich in einem vernünftigen Rahmen bewegen und unter dem Aspekt des Risikomanagements berechtigt sein; und

h. sich das vertragliche Recht auf Durchführung einzelner Prüfungen in ihrem Ermessen mit Blick auf die Auslagerung kritischer oder wesentlicher Funktionen vorbehalten.

94. In Einklang mit den Leitlinien der EBA für die IT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP) sollten die Institute, sofern angemessen, sicherstellen, dass sie Sicherheitspenetrationstests zur Bewertung der Wirksamkeit der durchgeführten Maßnahmen und Prozesse im Bereich Cyber-Sicherheit und interne IT-Sicherheit durchführen können. [36] Unter Berücksichtigung von Titel I sollten die Zahlungsinstitute zudem über interne IT-Kontrollmechanismen verfügen, einschließlich Kontrollmaßnahmen für die IT-Sicherheit und Maßnahmen zur Risikominderung.

95. Vor einer geplanten Vor-Ort-Prüfung sollten die Institute, Zahlungsinstitute, zuständigen Behörden und Prüfer oder im Namen des Instituts, Zahlungsinstituts oder zuständiger Behörden handelnde Dritte den Dienstleister angemessen informieren, es sei denn, dies ist aufgrund eines Notfalls oder einer Krisensituation nicht möglich oder würde zu einer Situation führen, in der die Prüfung nicht mehr wirksam ist.

96. Bei der Durchführung von Prüfungen in einer Mehrmandantenumgebung sollte darauf geachtet werden, dass Risiken für die Umgebung anderer Kunden (z. B. Auswirkungen auf die Dienstleistungsgüte, Verfügbarkeit von Daten, Vertraulichkeitsaspekte) vermieden oder gemindert werden.

97. Wenn die Auslagerungsvereinbarung mit einem hohen Maß an technischer Komplexität verbunden ist, beispielsweise im Fall von Cloud-Outsourcing, sollte das Institut oder das Zahlungsinstitut überprüfen, dass ungeachtet der mit der Durchführung der Prüfung beauftragten Personen – seien es eigene Prüfer, Prüfer bei Sammelprüfungen oder in seinem Namen handelnde externe Prüfer – über angemessene und einschlägige Kompetenzen und Kenntnisse für die wirksame Durchführung der entsprechenden Prüfungen und/oder Bewertungen verfügen. Dies gilt auch für Personal des Instituts oder Zahlungsinstituts, die Zertifizierungen von Dritten oder von Dienstleistern durchgeführte Prüfungen überprüfen.

13.4 Kündigungsrechte

98. In der Auslagerungsvereinbarung sollte für das Institut oder Zahlungsinstitut ausdrücklich die Möglichkeit vorgesehen sein, die Vereinbarung gemäß dem geltenden Gesetz zu kündigen, einschließlich in den folgenden Fällen:

    a. wenn der Dienstleister der ausgelagerten Funktionen gegen geltendes Recht, Rechtsvorschriften oder Vertragsbestimmungen verstößt;

    b. wenn Hindernisse, durch die die Durchführung der ausgelagerten Funktion verändert werden kann, ermittelt werden;

[36] Siehe auch EBA-Leitlinien für die IT-Risikobewertung: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

c. wenn wesentliche Änderungen auftreten, die sich auf die Auslagerungsvereinbarung oder den Dienstleister auswirken (z. B. eine Weiterverlagerung oder Änderungen bei den Subunternehmern);

d. wenn Mängel bezüglich des Umgangs mit und der Sicherheit von vertraulichen, personenbezogenen oder anderweitig sensiblen Daten oder Informationen auftreten; und

e. wenn Anweisungen durch die zuständige Behörde des Instituts oder des Zahlungsinstituts erteilt werden, beispielsweise wenn die zuständige Behörde aufgrund der Auslagerungsvereinbarung nicht mehr in der Lage ist, das Institut oder Zahlungsinstitut wirksam zu überwachen.

99. Die Auslagerungsvereinbarung sollte die Übertragung der ausgelagerten Funktion an einen anderen Dienstleister oder ihre Reintegration in das Institut oder Zahlungsinstitut ermöglichen. Zu diesem Zweck sollten in der schriftlichen Auslagerungsvereinbarung folgende Regelungen enthalten sein:

a. Festlegung der Pflichten des bestehenden Dienstleisters im Fall einer Übertragung der ausgelagerten Funktion an einen anderen Dienstleister oder der Reintegration in das Institut oder Zahlungsinstitut, einschließlich der Behandlung von Daten;

b. Festlegung eines angemessenen Übergangszeitraums, in dem der Dienstleister nach Kündigung der Auslagerungsvereinbarung weiterhin die ausgelagerte Funktion durchführt, um das Risiko von Unterbrechungen zu verringern; sowie

c. Aufnahme einer Pflicht des Dienstleisters zur Unterstützung des Instituts oder Zahlungsinstituts bei der ordnungsgemäßen Übertragung der Funktion im Fall einer Kündigung der Auslagerungsvereinbarung.

14 Beaufsichtigung der ausgelagerten Funktionen

100. Die Institute und Zahlungsinstitute sollten laufend die Leistung des Dienstleisters hinsichtlich aller Auslagerungsvereinbarungen nach einem risikobasierten Ansatz überwachen, wobei die Auslagerung von kritischen oder wesentlichen Funktionen den Schwerpunkt bildet; dies schließt auch mit ein, dass die Verfügbarkeit, Integrität und Sicherheit von Daten und Informationen gewährleistet sind. Wenn sich das Risiko, die Art oder der Umfang einer ausgelagerten Funktion erheblich geändert haben, sollten die Institute und Zahlungsinstitute die Kritikalität oder Wesentlichkeit der betreffenden Funktion in Einklang mit Abschnitt 4 neu bewerten.

101. Die Institute und Zahlungsinstitute sollten bei der Überwachung und Verwaltung von Auslagerungsvereinbarungen mit der gebotenen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit vorgehen.

102. Die Institute sollten regelmäßig ihre Risikobewertung gemäß Abschnitt 12.2 aktualisieren und dem Leitungsorgan in regelmäßigen Abständen über die in Zusammenhang mit der Auslagerung kritischer oder wesentlicher Funktionen ermittelten Risiken Bericht erstatten.

103. Die Institute und Zahlungsinstitute sollten ihre durch Auslagerungsvereinbarungen entstandenen internen Konzentrationsrisiken unter Berücksichtigung von Abschnitt 12.2 der vorliegenden Leitlinien überwachen und steuern.

104. Die Institute und Zahlungsinstitute sollten durch folgende Maßnahmen fortlaufend sicherstellen, dass Auslagerungsvereinbarungen angemessenen Leistungs- und Qualitätsstandards in Einklang mit ihren Richtlinien entsprechen, wobei ausgelagerte kritische oder wesentliche Funktionen den Schwerpunkt bilden:

a. Sicherstellung, dass sie angemessene Berichte von den Dienstleistern erhalten;

b. Bewertung der Leistung der Dienstleister mithilfe von Instrumenten wie zentralen Leistungsindikatoren, zentralen Kontrollindikatoren, Berichten über die Dienstleistungserbringung, Selbstzertifizierung und unabhängigen Überprüfungen; sowie

c. Überprüfung aller weiteren relevanten Informationen, die vom Dienstleister übermittelt werden, einschließlich Berichten über die Geschäftsfortführung und Tests.

105. Die Institute sollten geeignete Maßnahmen ergreifen, wenn sie Mängel bei der Durchführung der ausgelagerten Funktion feststellen. Insbesondere sollten die Institute und Zahlungsinstitute etwaigen Hinweisen nachgehen, dass die Dienstleister möglicherweise die ausgelagerte kritische oder wesentliche Funktion nicht wirksam oder in Einklang mit den geltenden Gesetzten und aufsichtlichen Anforderungen erfüllen. Falls Mängel ermittelt werden, sollten die Institute und Zahlungsinstitute geeignete Korrektur- oder Abhilfemaßnahmen ergreifen. Solche Maßnahmen können gegebenenfalls die fristlose Kündigung der Auslagerungsvereinbarung umfassen.

15 Ausstiegsstrategien

106. Bei der Auslagerung von kritischen oder wesentlichen Funktionen sollten die Institute und Zahlungsinstitute über eine dokumentierte Ausstiegsstrategie verfügen, die mit ihrer Auslagerungspolitik und den Plänen zur Geschäftsfortführung in Einklang stehen[37], wobei mindestens folgende Möglichkeit zu berücksichtigen ist:

a. die Kündigung der Auslagerungsvereinbarungen;

[37] In Einklang mit den Anforderungen nach Artikel 85 Absatz 2 der Richtlinie 2013/36/EU und Titel VI der Leitlinien der EBA zur internen Governance sollten die Institute und Zahlungsinstitute über geeignete Geschäftsfortführungspläne hinsichtlich der Auslagerung kritischer oder bedeutender Funktionen verfügen.

b. der Ausfall des Dienstleisters;

c. die Verschlechterung der Qualität der ausgeführten Funktion und tatsächliche oder potenzielle betriebliche Störungen aufgrund der unangemessenen oder unterlassenen Ausführung der Funktion;

d. Entstehen wesentlicher Risiken für die angemessene und fortlaufende Anwendung der Funktion.

107. Die Institute und Zahlungsinstitute sollten sicherstellen, dass sie in der Lage sind, Auslagerungsvereinbarungen zu beenden, ohne dass eine unverhältnismäßige Störung ihrer Geschäftstätigkeit auftritt, ohne ihre Erfüllung der aufsichtlichen Anforderungen einzuschränken und ohne die Kontinuität und Qualität der Bereitstellung von Dienstleistungen für die Kunden zu beeinträchtigen. Um dies zu erreichen, sollten sie

a. Ausstiegspläne entwickeln und umsetzen, die umfassend, dokumentiert und gegebenenfalls ausreichend erprobt sind (z. B. durch die Durchführung einer Analyse der potenziellen Kosten, Folgen, Mittel und zeitlichen Auswirkungen der Übertragung einer ausgelagerten Dienstleistung an einen anderen Anbieter); und

b. alternative Lösungen ermitteln und Übergangspläne entwickeln, um dem Institut oder Zahlungsinstitut zu ermöglichen, die ausgelagerten Funktionen und Daten dem Dienstleister zu entziehen und diese an alternative Anbieter zu übertragen bzw. wieder in das Institut oder Zahlungsinstitut einzugliedern oder andere Maßnahmen zu ergreifen, um die kontinuierliche Erfüllung der kritischen oder wesentlichen Funktion oder Geschäftstätigkeit in einer kontrollierten und ausreichend erprobten Art und Weise sicherzustellen, wobei den Herausforderungen Rechnung zu tragen ist, die durch den Standort der Daten entstehen können, und die erforderlichen Maßnahmen zu ergreifen sind, um die Betriebskontinuität in der Übergangsphase sicherzustellen.

108. Bei der Ausarbeitung von Ausstiegsstrategien sollten die Institute und Zahlungsinstitute folgende Gesichtspunkte einbeziehen:

a. Festlegung der Ziele der Ausstiegsstrategie;

b. Durchführung einer dem Risiko der ausgelagerten Prozesse, Dienstleistungen oder Tätigkeiten angemessenen Business-Impact-Analyse zur Feststellung, welche personellen und finanziellen Ressourcen zur Umsetzung des Ausstiegsplans erforderlich wären und wie lange dies dauern würde;

c. Zuweisung von Rollen, Zuständigkeiten und ausreichenden Mitteln zur Abwicklung von Ausstiegsplänen und Umstellungstätigkeiten;

d. Definition von Erfolgskriterien für die Umstellung der ausgelagerten Funktionen und Daten; sowie

e. Festlegung von Indikatoren, die für die Überwachung der Auslagerungsvereinbarung zugrunde gelegt werden (entsprechend den Ausführungen in Abschnitt 14), darunter auch Indikatoren für eine inakzeptable Dienstleistungsgüte, die zur Auslösung des Ausstiegsplans führen sollten.

Titel V – An die zuständigen Behörden gerichtete Leitlinien zu Auslagerungen

109. Bei der Festlegung geeigneter Methoden für die Überwachung der Einhaltung der Bedingungen für die ursprüngliche Zulassung durch die Institute und Zahlungsinstitute sollten die zuständigen Behörden überprüfen, ob Auslagerungsvereinbarungen zu einer erheblichen Veränderung der Bedingungen und Pflichten der ursprünglichen Zulassung der Institute und Zahlungsinstitute führen.

110. Die zuständigen Behörden sollten sich davon überzeugen, dass sie die Institute und Zahlungsinstitute wirksam überwachen können, einschließlich des Aspekts, dass die Institute und Zahlungsinstitute in ihrer Auslagerungsvereinbarung die Pflicht des Dienstleisters vorsehen, der zuständigen Behörde und dem Institut Prüfungs- und Zugangsrechte gemäß Abschnitt 13.3 zu gewähren.

111. Die Analyse der Auslagerungsrisiken der Institute sollte mindestens im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP) bzw. mit Blick auf Zahlungsinstitute als Teil anderer aufsichtlicher Prozesse, einschließlich Ad-hoc-Ersuchen, oder bei Kontrollen vor Ort erfolgen.

112. Zusätzlich zu den Informationen, die in dem in Abschnitt 11 erwähnten Register erfasst werden, können die zuständigen Behörden die Institute und Zahlungsinstitute um weitere Informationen ersuchen, insbesondere für kritische oder wesentliche Auslagerungsvereinbarungen, wie etwa:

a. die detaillierte Risikoanalyse:

b. ob der Dienstleister über einen Betriebskontinuitätsplan verfügt, der für die für das Institut oder Zahlungsinstitut erbrachten Dienstleistungen geeignet ist;

c. die heranzuziehende Ausstiegsstrategie, wenn die Auslagerungsvereinbarung von einer der Parteien gekündigt oder die Erbringung der Dienstleistungen unterbrochen wird; und

d. die vorhandenen Mittel und Maßnahmen zur angemessenen Überwachung der ausgelagerten Tätigkeiten.

113. Zusätzlich zu den nach Abschnitt 11 erforderlichen Informationen können die zuständigen Behörden die Institute und Zahlungsinstitute ersuchen, detaillierte Informationen über eine

Auslagerungsvereinbarung vorzulegen, selbst wenn die betreffende Funktion nicht als kritisch oder wesentlich betrachtet wird.

114. Die zuständigen Behörden sollten folgende Aspekte auf Grundlage eines risikobasierten Ansatzes bewerten:

a. ob die Institute und Zahlungsinstitute insbesondere kritische oder wesentliche Auslagerungsvereinbarungen angemessen überwachen und steuern;

b. ob die Institute und Zahlungsinstitute hinreichende Mittel für die Überwachung und das Management von Auslagerungsvereinbarungen zugewiesen haben;

c. ob die Institute und Zahlungsinstitute alle einschlägigen Risiken erkennen und steuern; und

d. ob die Institute und Zahlungsinstitute Interessenkonflikte mit Blick auf Auslagerungsvereinbarungen erkennen, bewerten und angemessen steuern, z. B. im Fall einer gruppeninternen Auslagerung oder einer Auslagerung im selben institutsbezogenen Sicherungssystem.

115. Die zuständigen Behörden sollten sicherstellen, dass Institute und Zahlungsinstitute in der EU/im EWR nicht als „leere Hüllen“ fungieren, dies schließt auch Fälle ein, in denen die Institute „Back-to-back-Transaktionen“ oder gruppeninterne Transaktionen nutzen, um einen Teil des Marktrisikos und des Kreditrisikos auf ein Unternehmen außerhalb der EU bzw. des EWR zu übertragen; zudem sollten sie sicherstellen, dass sie über angemessene Governance-Regelungen und Regelungen für das Risikomanagement zur Ermittlung und Steuerung ihrer Risiken verfügen.

116. Im Rahmen ihrer Bewertung sollten die zuständigen Behörden alle Risiken berücksichtigen, insbesondere:[38]

a. die mit der Auslagerungsvereinbarung verbundenen[39] operationellen Risiken;

b. Reputationsrisiken;

c. das „Step-in-Risiko“, aufgrund dessen die Rettung eines Dienstleisters durch das Institut erforderlich sein kann, im Fall bedeutender Institute;

d. Konzentrationsrisiken innerhalb des Instituts, einschließlich auf konsolidierter Basis, die durch mehrere Auslagerungsvereinbarungen mit einem einzelnen Dienstleister

[38] Für Institute im Geltungsbereich der Richtlinie 2013/36/EU, siehe auch die Leitlinien der EBA für die IT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP): https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Siehe auch die EBA-Leitlinien für die IT-Risikobewertung: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

oder eng miteinander verbundenen Dienstleistern oder mehrere Auslagerungsvereinbarungen im selben Geschäftsbereich entstehen;

e. Konzentrationsrisiken auf Sektorebene, z. B. wenn mehrere Institute oder Zahlungsinstitute einen einzelnen Dienstleister oder eine kleine Gruppe von Dienstleistern beauftragen;

f. den Umfang, in dem das auslagernde Institut oder Zahlungsinstitut den Dienstleister kontrolliert oder über Möglichkeiten zur Beeinflussung seiner Maßnahmen verfügt, die Verringerung von Risiken, die mit einem höheren Maß an Kontrollen einhergehen kann, und der Umstand, ob der Dienstleister unter die konsolidierte Aufsicht der Gruppe fällt; sowie

g. Interessenkonflikte zwischen dem Institut und dem Dienstleister.

117. Werden Konzentrationsrisiken ermittelt, sollten die zuständigen Behörden die Entwicklung dieser Risiken überwachen und sowohl ihre potenziellen Auswirkungen auf andere Institute und Zahlungsinstitute als auch die Stabilität des Finanzmarktes bewerten; die zuständigen Behörden sollten gegebenenfalls die Abwicklungsbehörde über neue potenziell kritische Funktionen[40] informieren, die im Zuge dieser Bewertung ermittelt werden.

118. Sofern Bedenken ermittelt werden, die zu der Schlussfolgerung führen, dass ein Institut oder Zahlungsinstitut nicht mehr über solide Governance Regelungen verfügt oder die aufsichtlichen Anforderungen nicht erfüllt, sollten die zuständigen Behörden geeignete Maßnahmen ergreifen, die auch die Begrenzung oder Einschränkung des Umfangs der ausgelagerten Funktionen oder das Erfordernis eines Ausstiegs aus einer oder mehreren Auslagerungsvereinbarungen umfassen können. Insbesondere kann unter Berücksichtigung der Notwendigkeit eines ununterbrochenen Geschäftsbetriebs des Instituts oder Zahlungsinstituts eine Kündigung von Verträgen verlangt werden, wenn die Aufsicht und Durchsetzung aufsichtlicher Anforderungen durch andere Maßnahmen nicht gewährleistet werden kann.

119. Die zuständigen Behörden sollten sich vergewissern, dass sie eine wirksame Aufsicht ausüben können, insbesondere wenn die Institute und Zahlungsinstitute kritische oder wesentliche Funktionen auslagern und diese außerhalb der EU/des EWR durchgeführt werden.

[40] Entsprechend der Definition in Artikel 2 Absatz 1 Unterabsatz 35 BRRD.