EBA/GL/2022/15

22. November 2022

Leitlinien

zur Nutzung von Anwendungen für den Fern-Kundenannahmeprozess gemäß Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849

1. Einhaltung der Leitlinien und Meldepflichten

Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010[1] erlassen wurden. Gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Maßnahmen 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. Dazu sollten die zuständigen Behörden gemäß Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, und zwar auch dann, wenn bestimmte Leitlinien in erster Linie an die Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 30.05.2023 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Meldung ein, geht die EBA davon aus, dass die zuständige Behörde den Leitlinien nicht nachkommt. Die Meldungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars „EBA/GL/2022/15“ zu übermitteln. Die Meldungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer zuständigen Behörde zu übermitteln. Jegliche Änderungen des Konformitätsstatus müssen der EBA ebenfalls gemeldet werden.

4. Die Mitteilungen werden gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 auf der Website der EBA veröffentlicht.

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

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

5. In diesen Leitlinien werden die Schritte dargelegt, die Kredit- und Finanzinstitute bei der Einführung oder Überprüfung von Anwendungen ergreifen sollten, um ihren Verpflichtungen gemäß Artikel 13 Absatz 1 Buchstaben a, b und c der Richtlinie (EU) 2015/849 [2] beim Fern-Kundeannahmeprozess nachzukommen. Ferner werden darin die Schritte festgelegt, die die Kredit- und Finanzinstitute unternehmen sollten, wenn sie gemäß Kapitel I Abschnitt 4 der Richtlinie (EU) 2015/849 auf Dritte zurückgreifen, sowie die Strategien, Kontrollen und Verfahren dargelegt, die die Kredit- und Finanzinstitute im Hinblick auf die Sorgfaltspflichten gegenüber Kunden gemäß Artikel 8 Absatz 3 und Artikel 8 Absatz 4 Buchstabe a der Richtlinie (EU) 2015/849 einführen sollten, wenn die Anwendung der Sorgfaltspflichten gegenüber Kunden nicht vor Ort erfolgt.

6. Die zuständigen Behörden sollten diese Leitlinien berücksichtigen, wenn sie bewerten, ob die Maßnahmen, die Kredit- und Finanzinstitute ergreifen, um ihren Verpflichtungen gemäß der Richtlinie (EU) 2015/849 im Rahmen des Fern-Kundenannahmeprozesses nachzukommen, angemessen und wirksam sind.

Adressaten

7. Diese Leitlinien richten sich an zuständige Behörden im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010. Zudem richten sich diese Leitlinien an Akteure des Finanzsektors im Sinne von Artikel 4 Absatz 1a der genannten Verordnung, bei denen es sich um Kredit- und Finanzinstitute im Sinne von Artikel 3 Absätze 1 und 2 der Richtlinie (EU) 2015/849 handelt.

[2] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

Begriffsbestimmungen

8. Sofern nicht anders angegeben, haben die in der Richtlinie (EU) 2015/849 verwendeten und definierten Begriffe in den Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

Biometrische Daten	Personenbezogene Daten zu physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die deren eindeutige Identifizierung ermöglichen oder bestätigen, wie Gesichtsbilder oder Fingerabdruckdaten, die mithilfe technischer Mittel erhoben und verarbeitet werden.

3. Umsetzung

Geltungsbeginn

Diese Leitlinien gelten ab dem 02.10.2023.

4. Leitlinien zur Nutzung von Anwendungen für den Fern-Kundenannahmeprozess gemäß Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849

4.1 Interne Strategien und Verfahren

4.1.1 Strategien und Verfahren für den Fern-Kundenannahmeprozess

9. Die Kredit- und Finanzinstitute sollten Strategien und Verfahren einführen und aufrechterhalten, um ihren Verpflichtungen gemäß Artikel 13 Absatz 1 Buchstaben a und c der Richtlinie (EU) 2015/849 in Fällen nachzukommen, in denen der Kundenannahmeprozessaus der Ferne erfolgt. Diese Strategien und Verfahren sollten risikoorientiert sein und mindestens Folgendes umfassen:

    a) eine allgemeine Beschreibung der Anwendung, die die Kredit- und Finanzinstitute für die Erhebung, Überprüfung und Aufzeichnung von Informationen während des gesamten Fern-Kundenannahmeprozesses eingeführt haben. Dies sollte eine Erläuterung der Merkmale und der Funktionsweise der Anwendung umfassen;

    b) die Fälle, in denen die Anwendung für den Fern-Kundenannahmeprozess genutzt werden kann, wobei die gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2015/849 und im Zuge der unternehmensweiten Risikobewertung ermittelten und bewerteten Risikofaktoren berücksichtigt werden, einschließlich einer Beschreibung der Kategorie von Kunden, Produkten und Dienstleistungen, die für den Fern-Kundenannahmeprozess infrage kommen;

    c) welche Schritte vollständig autonomisiert sind und für welche Schritte das Eingreifen einer Person erforderlich ist;

    d) die bestehenden Kontrollen, mit denen sichergestellt wird, dass die erste Transaktion mit einem neuen Kunden erst ausgeführt wird, wenn alle anfänglichen Maßnahmen zur Erfüllung der Sorgfaltspflichten gegenüber dem Kunden durchgeführt wurden;

    e) eine Beschreibung der Einführungsschulungen und regelmäßigen Schulungsprogramme, mit denen sichergestellt wird, dass das Personal sensibilisiert ist und aktuelle Kenntnisse über die Funktionsweise der Anwendung für den Fern-

Kundenannahmeprozessbesitzt sowie damit verbundenen Risiken, Strategien und Verfahren für den Fern-Kundenannahmeprozess, mit denen diese Risiken begrenzt werden sollen, besitzt.

10. Durch die Umsetzung der Strategien und Verfahren sollte es den Kredit- und Finanzinstituten möglich sein, die Einhaltung der Bestimmungen der Abschnitte 4.2 bis 4.7 dieser Leitlinien sicherzustellen.

4.1.2 Governance

11. Zusätzlich zu den Bestimmungen in Abschnitt 4.2.4 der EBA-Leitlinien bezüglich des Geldwäschebeauftragten[3] sollte der Geldwäschebeauftragte[4] im Rahmen seiner allgemeinen Pflicht zur Ausarbeitung von Strategien und Verfahren für die Erfüllung der Sorgfaltspflichten gegenüber Kunden sicherstellen, dass die Strategien und Verfahren für den Fern-Kundenannahmeprozess wirksam umgesetzt, regelmäßig überprüft und gegebenenfalls geändert werden.

12. Das Leitungsorgan des Kredit- und Finanzinstituts sollte Strategien und Verfahren für den Fern-Kundenannahmeprozess genehmigen und ihre ordnungsgemäße Umsetzung überwachen.

4.1.3 Die Bewertung vor der Einführung der Anwendung für den Fern-Kundenannahmeprozess

13. Wenn die Kredit- und Finanzinstitute prüfen, ob sie eine neue Anwendung für den Fern-Kundenannahmeprozess einführen wollen, sollten sie vor der Einführung eine Bewertung der Anwendung für den Fern-Kundenannahmeprozess vornehmen.

14. Die Kredit- und Finanzinstitute sollten in ihren Strategien und Verfahren den Umfang, die Schritte und die Aufzeichnungsanforderungen der Bewertung vor der Einführung festlegen, die mindestens Folgendes umfassen sollte:

    a) eine Bewertung der Angemessenheit der Anwendung hinsichtlich der Vollständigkeit und Genauigkeit der zu erhebenden Daten und einzuholenden Dokumente sowie der Zuverlässigkeit und der Unabhängigkeit der verwendeten Informationsquellen;

    b) eine Bewertung der Auswirkungen der Nutzung der Anwendung für den Fern-Kundenannahmeprozess auf die unternehmensweiten Risiken, einschließlich der Risiken hinsichtlich Geldwäsche und Terrorismusfinanzierung, operationeller und rechtlicher Risiken sowie Reputationsrisiken;

[3] Entwurf der Leitlinien zu Strategien und Verfahren in Bezug auf das Compliance-Management und die Rolle und Zuständigkeiten des Geldwäschebeauftragten gemäß Artikel 8 und Kapitel VI der Richtlinie (EU) 2015/849.

[4] Im Einklang mit den Kriterien der Verhältnismäßigkeit in Abschnitt 4.2.2 der Leitlinien bezüglich des Geldwäschebeauftragten.

c) die Ermittlung möglicher risikomindernder Maßnahmen und Abhilfemaßnahmen für jedes Risiko, das im Zuge der Bewertung gemäß Buchstabe b festgestellt wurde;

d) Tests zur Beurteilung von Betrugsrisiken, einschließlich des Risikos der Identitätserschleichung und anderer Risiken in Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) sowie Sicherheitsrisiken, gemäß Absatz 43 der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken[5];

e) End-to-End-Tests der Funktionsweise der Anwendung hinsichtlich Kunden-, Produkt- und Dienstleistungsstruktur(en), die in den Strategien und Verfahren für den Fern-Kundenannahmeprozess ermittelt wurde.

15. Die Kredit- und Finanzinstitute sollten die in Absatz 14 Buchstaben a, d und e genannten Kriterien als erfüllt betrachten, wenn der Anwendung eine der folgenden Optionen zugrunde liegt:

a) elektronische Identifizierungssysteme, die gemäß Artikel 9 der Verordnung (EU) Nr. 910/2014 notifiziert wurden und die Anforderungen an die Sicherheitsniveaus „substanziell“ bzw. „hoch“ gemäß Artikel 8 dieser Verordnung erfüllen;

b) relevante qualifizierte Vertrauensdienste, die die Anforderungen der Verordnung (EU) Nr. 910/2014, insbesondere Kapitel III Abschnitt 3 und Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe b der genannten Verordnung erfüllen.

16. Die Kredit- und Finanzinstitute sollten in der Lage sein, der für sie zuständigen Behörde nachzuweisen, welche Beurteilungen sie vor der Einführung der Anwendung für den Fern-Kundenannahmeprozess durchgeführt haben, welche Ergebnisse ihre Beurteilungen erzielt hat und ob die Anwendung das Geldwäsche- und Terrorismusfinanzierungsrisiko hinsichtlich ihrer Kunden-, Dienstleistungs-, Produktstruktur sowie bezüglich der geografischen Tätigkeitsgebiete angemessen adressiert.

17. Die Kredit- und Finanzinstitute sollten erst dann mit der Nutzung einer Anwendung für den Fern-Kundenannahmeprozess beginnen, wenn sie sich davon überzeugt haben, dass sie in das umfassendere interne Kontrollsystem des Instituts integriert werden kann, sodass das Institut die Risiken hinsichtlich Geldwäsche und Terrorismusfinanzierung, die sich aus der Nutzung der Anwendung für den Fern-Kundenannahmeprozess ergeben können, angemessen steuern kann.

4.1.4 Laufende Überwachung der Anwendung für den Fern-Kundenannahmeprozess

18. Die Kredit- und Finanzinstitute sollten die Anwendung für den Fern-Kundenannahmeprozess kontinuierlich überwachen, um sicherzustellen, dass sie entsprechend den Erwartungen der

[5] EBA/GL/2019/04.

Kredit- und Finanzinstitute funktioniert. Sie sollten ihre in Absatz 9 beschriebenen Strategien und Verfahren durch eine Beschreibung mindestens folgender Elemente ergänzen:

a) die Schritte, die sie unternehmen werden, um sich von der kontinuierlichen Qualität, Vollständigkeit, Genauigkeit und Angemessenheit der während des Verfahrens für den Fern-Kundenannahmeprozess erhobenen Daten zu überzeugen, die auf die Risiken hinsichtlich Geldwäsche und Terrorismusfinanzierung abgestimmt sein sollten, denen das Kredit- und Finanzinstitut ausgesetzt ist;

b) Umfang und Häufigkeit dieser regelmäßigen Überprüfungen sowie

c) die Umstände, unter denen Ad-hoc-Überprüfungen durchgeführt werden; diese sollten mindestens Folgendes einschließen:

   a. Änderungen des Risikos hinsichtlich Geldwäsche und Terrorismusfinanzierung, dem das Kredit- und Finanzinstituts ausgesetzt ist;

   b. Mängel bei der Funktionsweise der Anwendung, die im Rahmen von Überwachungs-, Prüfungs- oder Aufsichtstätigkeiten festgestellt werden;

   c. eine wahrgenommene Zunahme von Betrugsversuchen;

   d. Änderungen des Rechts- oder Aufsichtsrahmens.

19. Die Kredit- und Finanzinstitute sollten in ihren Verfahren und Prozessen Abhilfemaßnahmen für den Fall vorsehen, dass ein Risiko eingetreten ist oder Fehler festgestellt wurden, die sich auf die Effizienz und Wirksamkeit der allgemeinen Anwendung für den Fern-Kundenannahmeprozess auswirken. Diese Maßnahmen sollten mindestens Folgendes umfassen:

a) eine Überprüfung aller betroffenen Geschäftsbeziehungen, um zu bewerten, ob die Kredit- und Finanzinstitute anfänglich in ausreichendem Maße ihre Sorgfaltspflicht bei der Feststellung der Kundenidentität erfüllt haben, um den Bestimmungen in Artikel 13 Absatz 1 Buchstaben a, b und c der Geldwäscherichtlinie zu entsprechen. Die Kredit- und Finanzinstitute sollten den Geschäftsbeziehungen Vorrang einräumen, die mit dem höchsten Risiko hinsichtlich Geldwäsche und Terrorismusfinanzierung verbunden sind;

b) unter Berücksichtigung der im Rahmen der oben genannten Überprüfung eingeholten Informationen eine Bewertung, ob die betroffenen Geschäftsbeziehungen

   a. zusätzlichen Sorgfaltspflichten unterliegen sollten;

b. Beschränkungen unterliegen sollten, wie z. B. Obergrenzen für das Transaktionsvolumen, sofern dies nach nationalem Recht zulässig ist, bis eine Überprüfung stattgefunden hat;

c. beendet werden sollten;

d. der FIU gemeldet werden sollten;

e. in eine andere Risikokategorie umgestuft werden sollten.

20. Die Kredit- und Finanzinstitute sollten den wirksamsten Weg in Erwägung ziehen, um die dauerhafte Angemessenheit und Zuverlässigkeit der Anwendungen für den Fern-Kundenannahmeprozess zu überwachen. Sie sollten unter anderem eines oder mehrere der folgenden Instrumente in Betracht ziehen:

i. Qualitätssicherungsprüfungen;

ii. automatisierte kritische Warnungen und Meldungen;

iii. regelmäßige automatisierte Qualitätsberichte;

iv. Stichprobenprüfungen;

v. manuelle Überprüfungen.

21. Dieser Abschnitt gilt auch, wenn voll automatisierte Anwendungen für den Fern-Kundenannahmeprozess eingesetzt werden, die in hohem Maße von automatisierten Algorithmen abhängig sind und die kaum oder kein menschliches Eingreifen erfordern.

22. Die Kredit- und Finanzinstitute sollten in der Lage sein, ihrer zuständigen Behörde nachzuweisen, welche Überprüfungen sie durchgeführt und welche Abhilfemaßnahmen sie ergriffen haben, um während der Nutzungsdauer der Anwendung für den Fern-Kundenannahmeprozess festgestellte Mängel zu beheben.

4.2 Informationsbeschaffung

4.2.1 Feststellung der Identität des Kunden

23. Zusätzlich zu den in Absatz 9 genannten Punkten sollten die Kredit- und Finanzinstitute in ihren Strategien und Verfahren die zur Feststellung der Identität des Kunden erforderlichen Informationen, die Arten von Dokumenten, Daten oder Informationen, die das Institut zur Überprüfung der Identität des Kunden verwendet, und die Art und Weise, wie diese Informationen überprüft werden, darlegen.

24. Die Kredit- und Finanzinstitute sollten sicherstellen, dass

a) die im Rahmen der Anwendung für den Fern-Kundenannahmeprozess eingeholten Informationen aktuell und angemessen sind, um die geltenden Rechtsvorschriften und Regulierungsstandards für die anfängliche Sorgfaltspflicht bei der Feststellung der Kundenidentität zu erfüllen;

b) Bilder, Videos, Ton und Daten in einem lesbaren Format und in ausreichender Qualität erfasst werden, sodass der Kunde eindeutig zu erkennen ist;

c) das Verfahren zur Feststellung der Identität des Kunden nicht fortgesetzt wird, wenn technische Mängel oder unerwartete Verbindungsunterbrechungen festgestellt werden.

25. Die Kredit- und Finanzinstitute sollten die in Absatz 24 genannten Kriterien als erfüllt betrachten, wenn der Anwendung eine der folgenden Optionen zugrunde liegt:

a) elektronische Identifizierungssysteme, die gemäß Artikel 9 der Verordnung (EU) Nr. 910/2014 notifiziert wurden und die Anforderungen an die Sicherheitsniveaus „substanziell“ bzw. „hoch“ gemäß Artikel 8 dieser Verordnung erfüllen;

b) relevante qualifizierte Vertrauensdienste, die die Anforderungen der Verordnung (EU) Nr. 910/2014, insbesondere Kapitel III Abschnitt 3 und Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe b der genannten Verordnung erfüllen.

26. Die im Zuge der Fernidentifizierung eingeholten Dokumente und Informationen, die gemäß Artikel 40 Absatz 1 Buchstabe a der Richtlinie (EU) 2015/849 aufbewahrt werden müssen, sollten von dem Kredit- und Finanzinstitut mit einem Zeitstempel versehen und sicher gespeichert werden. Der Inhalt gespeicherter Aufzeichnungen, einschließlich Bildern, Videos, Ton und Daten, sollte in einem lesbaren Format verfügbar sein, und es sollten nachträgliche Überprüfungen möglich sein.

4.2.2 Identifizierung natürlicher Personen

27. Die Kredit- und Finanzinstitute sollten in ihren Strategien gemäß Abschnitt 4.1.1 Absatz 9 festlegen, welche Informationen sie benötigen, um eine Fernidentifizierung der Kunden im Einklang mit Artikel 13 Absatz 1 Buchstaben a und c der Richtlinie (EU) 2015/849 durchzuführen. Darüber hinaus sollten die Kredit- und Finanzinstitute festlegen, welche Informationen

a) vom Kunden manuell eingegeben werden;

b) automatisch aus den vom Kunden bereitgestellten Dokumenten erfasst werden;

c) anhand anderer interner oder externer Quellen erhoben werden.

28. Die Kredit- und Finanzinstitute sollten geeignete Mechanismen einrichten und aufrechterhalten, um sicherzustellen, dass die gemäß Absatz 27 automatisch erfassten

Informationen zuverlässig sind. Sie sollten Kontrollen durchführen, um den damit verbundenen Risiken Rechnung zu tragen, einschließlich Risiken im Zusammenhang mit der automatischen Erfassung von Daten, wie der Verschleierung des Standorts des Geräts des Kunden, gefälschte Internetprotokoll (IP)-Adressen oder Dienste wie virtuelle private Netze (VPN).

4.2.3 Identifizierung von juristischen Personen

29. Wenn die Kredit- und Finanzinstitute eine Geschäftsbeziehung mit Kunden, bei denen es sich um juristische Personen handelt, aus der Ferne aufnehmen, sollten sie in ihren Strategien und Verfahren gemäß Abschnitt 4.1.1 Absatz 9 festlegen, für welche Kategorie von juristischen Personen sie den Fern-Kundenannahmeprozess durchführen, wobei das mit den einzelnen Kategorien verbundene Risiko hinsichtlich Geldwäsche und Terrorismusfinanzierung und der für die Validierung der Angaben zur Identität erforderliche Umfang des menschlichen Eingreifens zu berücksichtigen sind.

30. Die Kredit- und Finanzinstitute sollten sicherstellen, dass die Anwendung für den Fern-Kundenannahmeprozess über Funktionen verfügt, mit denen Folgendes erfasst werden kann:

    a) alle relevanten Daten und Unterlagen zur Identifizierung und Überprüfung der juristischen Person

    b) alle relevanten Daten und Unterlagen zur Überprüfung, ob die im Namen der juristischen Person auftretende natürliche Person rechtlich befugt ist, als solche zu handeln;

    c) die Angaben zu den wirtschaftlichen Eigentümern gemäß Abschnitt 4.12 der EBA-Leitlinien zu den Risikofaktoren[6].

31. Bei natürlichen Personen, die im Namen einer juristischen Person handeln, sollten die Kredit- und Finanzinstitute das in Abschnitt 4.2.2 beschriebene Verfahren zur Feststellung der Identität anwenden.

4.2.4 Art und Zweck der Geschäftsbeziehung

32. Wenn die Kredit- und Finanzinstitute gemäß Artikel 13 Absatz 1 Buchstabe c der Richtlinie (EU) 2015/849 und entsprechend den Ausführungen in Abschnitt 4.38 der EBA-Leitlinien zu den Risikofaktoren den Zweck und die angestrebte Art der Geschäftsbeziehung bewerten und gegebenenfalls Informationen über diese einholen, sollten sie für die Zwecke dieser Leitlinien die entsprechenden Maßnahmen vor dem Ende des Verfahrens zum Fern-Kundenannahmeprozess abgeschlossen haben.

[6] EBA/GL/2021/02.

4.3 Echtheit und Integrität der Dokumente

33. Wenn die Kredit- und Finanzinstitute Kopien eines Originaldokuments akzeptieren und das Original nicht prüfen, sollten sie Maßnahmen ergreifen, um sicherzustellen, dass die Kopie zuverlässig ist. Die Kredit- und Finanzinstitute sollten mindestens Folgendes vorsehen:

    a) einen Vergleich mit amtlichen Datenbanken wie PRADO[7],wenn die Kopie in das Originaldokument integrierte Sicherheitsmerkmale enthält und die Spezifikationen des vervielfältigten Originaldokuments gültig und akzeptabel sind, insbesondere hinsichtlich der Art, Größe der Zeichen und Struktur des Dokuments;

    b) Überprüfung, ob personenbezogene Daten verändert oder anderweitig manipuliert wurden oder gegebenenfalls ob das in das Dokument eingebettete Bild des Kunden ersetzt wurde;

    c) Überprüfung der Integrität des Algorithmus zur Generierung der eindeutigen Kennnummer des Originaldokuments, falls das amtliche Dokument mit einer maschinenlesbaren Zone (MLZ) ausgestellt wurde;

    d) Überprüfung, ob die vorgelegte Kopie von hinreichender Qualität und die Auflösung ausreichend ist, um sicherzustellen, dass die relevanten Informationen eindeutig sind;

    e) Überprüfung, dass die vorgelegte Kopie nicht auf Grundlage eines Fotos oder Scans des ursprünglichen Ausweisdokuments auf einem Bildschirm angezeigt wird.

34. Wenn die Kredit- und Finanzinstitute Funktionen nutzen, um Informationen aus Dokumenten automatisch zu lesen, wie z. B. Algorithmen für die maschinelle optische Zeichenerkennung (OZE) oder Überprüfungen von maschinenlesbaren Zonen (MLZ), sollten sie die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass diese Instrumente die Informationen korrekt und einheitlich erfassen.

35. In Fällen, in denen das Gerät, das die Kunden zum Nachweis ihrer Identität verwenden, die Erhebung relevanter Daten ermöglicht, z. B., weil die Daten auf dem Chip eines nationalen Ausweisdokuments enthalten sind, und es für Kredit- und Finanzinstitute technisch machbar ist, auf diese Daten zuzugreifen, sollten die Kredit- und Finanzinstitute die Verwendung dieser Informationen in Erwägung ziehen, um ihre Übereinstimmung mit den Informationen zu überprüfen, die aus anderen Quellen, wie den übermittelten Daten oder anderen vom Kunden vorgelegten Dokumenten, erhoben wurden.

36. Sofern verfügbar, sollten die Kredit- und Finanzinstitute während des Überprüfungsverfahrens die Sicherheitsmerkmale, mit denen das amtliche Dokument

[7] https://www.consilium.europa.eu/prado/en/prado-start-page.html.

gegebenenfalls zum Nachweis seiner Echtheit versehen ist, wie z. B. Hologramme, überprüfen.

37. Die Kredit- und Finanzinstitute sollten in ihren Strategien und Verfahren festlegen, wie sie ihre Dokumentationsanforderungen für die Zwecke der Inklusion in das Finanzsystem anpassen. Sofern in der Folge schwächere oder nicht herkömmliche Formen der Dokumentation akzeptiert werden, sollten die Kredit- und Finanzinstitute zusätzlich zu den in Absatz 4.10 der EBA-Leitlinien zu den Risikofaktoren genannten Maßnahmen Kontrollen oder ein verstärktes menschliches Eingreifen vorsehen, um sich davon zu überzeugen, dass sie das mit der Geschäftsbeziehung verbundene Risiko hinsichtlich Geldwäsche und Terrorismusfinanzierung verstehen.

4.4 Abgleich der Kundenidentität im Rahmen des Überprüfungsverfahrens

38. Die von den Kredit- und Finanzinstituten implementierten Anwendungen für den Fern-Kundenannahmeprozess sollten im Rahmen des Überprüfungsverfahrens mindestens folgende Kontrollen ermöglichen:

    a) ob die sichtbaren Informationen über die natürliche Person mit den vorgelegten Unterlagen übereinstimmen;

    b) wenn es sich bei dem Kunden um eine juristische Person handelt, ob diese gegebenenfalls in ein öffentliches Register eingetragen ist;

    c) wenn es sich bei dem Kunden um eine juristische Person handelt, ob die natürliche Person, die sie vertritt, berechtigt ist, in ihrem Namen zu handeln.

39. Wenn die Anwendung für den Fern-Kundenannahmeprozess die Verwendung biometrischer Daten zur Überprüfung der Identität des Kunden einschließt, sollten die Kredit- und Finanzinstitute sicherstellen, dass die biometrischen Daten ausreichend eindeutig sind, um sie unmissverständlich einer einzigen natürlichen Person zuzuordnen. Die Kredit- und Finanzinstitute sollten leistungsstarke und zuverlässige Algorithmen verwenden, um die Übereinstimmung zwischen den biometrischen Daten, die auf dem übermittelten Ausweisdokument angegeben sind, und dem neuen Kunden, mit dem eine Geschäftsbeziehung aufgenommen wird, zu überprüfen. In Fällen, in denen die Anwendung nicht das erforderliche Maß an Zuverlässigkeit bietet, sollten zusätzliche Kontrollen durchgeführt werden.

40. Wenn die vorgelegten Nachweise von unzureichender Qualität sind, was zu Unklarheiten oder Unsicherheiten führt, sodass die Durchführung von Fernkontrollen beeinträchtigt wird, sollte das jeweilige Verfahren zum Fern-Kundenannahmeprozess unterbrochen und erneut eingeleitet oder zu einer persönlichen Überprüfung weiterverwiesen werden.

41. Wenn die Kredit- und Finanzinstitute unbegleitete Anwendungen für den Fern-Kundenannahmeprozess nutzen, bei denen der Kunde im Rahmen des Überprüfungsverfahrens nicht mit einem Mitarbeiter interagiert, sollten sie

    a) sicherstellen, dass Fotos oder Videos unter angemessenen Lichtverhältnissen aufgenommen werden und dass die erforderlichen Merkmale mit der notwendigen Klarheit erfasst werden, damit die Identität des Kunden ordnungsgemäß überprüft werden kann;

    b) sicherstellen, dass alle Fotos oder Videoaufnahmen zu dem Zeitpunkt aufgenommen werden, zu dem der Kunde das Überprüfungsverfahren durchführt;

    c) eine Lebendigkeitserkennung durchführen, die Verfahren einschließen kann, bei denen eine bestimmte Handlung des Kunden erforderlich ist, um zu überprüfen, ob er tatsächlich anwesend ist, oder die auf der Analyse der erhaltenen Daten basieren kann, ohne dass eine spezifische Handlung des Kunden erforderlich ist;

    d) leistungsstarke und zuverlässige Algorithmen verwenden, um zu überprüfen, ob die Fotos oder Videoaufnahmen mit den Bildern übereinstimmen, die aus dem amtlichen Dokument oder den amtlichen Dokumenten des Kunden abgerufen wurden.

42. Wenn die Kredit- und Finanzinstitute begleitete Anwendungen für den Fern-Kundenannahmeprozess nutzen, bei denen der Kunde im Rahmen des Überprüfungsverfahrens mit einem Mitarbeiter interagiert, sollten sie

    a) sicherstellen, dass die Bild- und Audioqualität ausreichend ist, um eine ordnungsgemäße Überprüfung der Identität des Kunden zu ermöglichen, und dass zuverlässige technische Systeme eingesetzt werden;

    b) die Mitwirkung eines Mitarbeiters vorsehen, der über ausreichende Kenntnisse der geltenden Verordnung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und der Sicherheitsaspekte der Fernüberprüfung verfügt sowie ausreichend geschult ist, um den vorsätzlichen oder absichtlichen Einsatz von Täuschungstechniken im Zusammenhang mit einer Fernüberprüfung zu antizipieren und zu verhindern und im Falle eines solchen Vorgehens zu reagieren;

    c) einen Interviewleitfaden ausarbeiten, in dem die weiteren Schritte im Rahmen der Fernüberprüfung sowie die vom Mitarbeiter durchzuführenden Maßnahmen festgelegt werden. Der Interviewleitfaden sollte Leitlinien für die Beobachtung und Ermittlung psychologischer Faktoren oder anderer Merkmale enthalten, die für verdächtiges Verhalten bei der Fernüberprüfung kennzeichnend sein können.

43. Sofern möglich, sollten Kredit- und Finanzinstitute Anwendungen für den Fern-Kundenannahmeprozess nutzen, die Zufälligkeit bei der Reihenfolge der vom Kunden zu

Überprüfungszwecken durchzuführenden Maßnahmen einschließt, um sich gegen Risiken wie die Verwendung synthetischer Identitäten oder Nötigung zu schützen. Sofern möglich, sollten die Kredit- und Finanzinstitute dem für die Fernüberprüfung verantwortlichen Mitarbeiter auch Aufträge nach dem Zufallsprinzip erteilen, um Absprachen zwischen dem Kunden und dem verantwortlichen Mitarbeiter zu vermeiden.

44. Darüber hinaus sollten die Kredit- und Finanzinstitute zur Verbesserung der Zuverlässigkeit des Überprüfungsverfahrens eine oder mehrere der nachfolgend genannten Kontrollen oder eine vergleichbare Maßnahme anwenden, sofern sie dem mit der Geschäftsbeziehung verbundenen Risiko hinsichtlich Geldwäsche und Terrorismusfinanzierung angemessen sind. Diese Kontrollen oder Maßnahmen können unter anderem Folgendes einschließen:

    a) Die erste Zahlung erfolgt über ein Einzel- oder Gemeinschaftskonto des Kunden bei einem regulierten Kredit- oder Finanzinstitut mit Sitz innerhalb des EWR oder in einem Drittland, dessen Anforderungen an die Bekämpfung von Geldwäsche und Terrorismusfinanzierung mindestens den Vorgaben der Richtlinie (EU) 2015/849 entsprechen.

    b) Dem Kunden wird ein nach dem Zufallsprinzip erstelltes Passwort übermittelt, um die Anwesenheit während der Fernüberprüfung zu bestätigen. Das Passwort sollte ein einmalig zu verwendender und zeitlich begrenzter Code sein.

    c) Es werden biometrische Daten erfasst, um sie mit Daten zu vergleichen, die über andere unabhängige und zuverlässige Quellen erhoben wurden.

    d) Telefonkontakte mit dem Kunden.

    e) Direktmailings (elektronisch und per Post) an den Kunden.

45. Die Kredit- und Finanzinstitute sollten die in den Absätzen 38 bis 43 genannten Kriterien als erfüllt betrachten, wenn der Anwendung eine der folgenden Optionen zugrunde liegt:

    a) elektronische Identifizierungssysteme, die gemäß Artikel 9 der Verordnung (EU) Nr. 910/2014 notifiziert wurden und die Anforderungen an die Sicherheitsniveaus „substanziell“ bzw. „hoch“ gemäß Artikel 8 dieser Verordnung erfüllen;

    b) relevante qualifizierte Vertrauensdienste, die die Anforderungen der Verordnung (EU) Nr. 910/2014, insbesondere Kapitel III Abschnitt 3 und Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe b der genannten Verordnung erfüllen.

4.5 Inanspruchnahme Dritter und Auslagerung

46. Zusätzlich zu den in Absatz 9 genannten Punkten sollten die Kredit- und Finanzinstitute in ihre Strategien und Verfahren Spezifikationen aufnehmen, in denen festgelegt wird, welche Funktionen und Tätigkeiten im Rahmen des Fern-Kundenannahmeprozesses von dem Kredit-

und Finanzinstitut, von Dritten oder von einem anderen externen Dienstleister wahrgenommen oder ausgeführt werden.

4.5.1 Rückgriff auf Drittanbieter gemäß Kapitel II Abschnitt 4 der Richtlinie (EU) 2015/849

47. Zusätzlich zu den EBA-Leitlinien zu den Risikofaktoren[8], insbesondere den Leitlinien 2.20 bis 2.21 sowie 4.32 bis 4.37 dieser Leitlinien, sollten sie die folgenden Kriterien anwenden:

    a) Ergreifen der erforderlichen Schritte, um sich zu vergewissern, dass die eigenen Prozesse und Verfahren des Drittanbieters im Hinblick auf die Sorgfaltspflichten gegenüber Kunden beim Fern-Kundenannahmeprozess sowie die Informationen und Daten, die er in diesem Zusammenhang erhebt, ausreichend sind und den Anforderungen dieser Leitlinien entsprechen;

    b) Gewährleistung der Weiterführung der Geschäftsbeziehungen zwischen dem Kunden und dem Kredit- und Finanzinstitut, um sich vor Ereignissen zu schützen, die Mängel bei dem von dem Dritten durchgeführten Verfahren zum Fern-Kundenannahmeprozess aufdecken könnten.

4.5.2 Auslagerung von Sorgfaltspflichten gegenüber Kunden

48. Wenn die Kredit- und Finanzinstitute das Verfahren zum Fern-Kundenannahmeprozess ganz oder teilweise an einen externen Dienstleister gemäß Artikel 29 der Richtlinie (EU) 2015/849 auslagern, sollten die Kredit- und Finanzinstitute zusätzlich zu den Leitlinien 2.20 bis 2.21 sowie 4.32 bis 4.37 der EBA-Leitlinien zu den Risikofaktoren sowie gegebenenfalls zusätzlich zu den EBA-Leitlinien zu Auslagerungen[9] vor und während der Geschäftsbeziehung mit dem externen Dienstleister die folgenden Maßnahmen anwenden, deren Umfang auf risikoorientierter Grundlage angepasst werden sollte:

    a) Gewährleistung, dass der externe Dienstleister die Strategien und Verfahren des Kredit- und Finanzinstituts für den Fern-Kundenannahmeprozess im Einklang mit der Auslagerungsvereinbarung wirksam umsetzt und einhält. Dies sollte durch regelmäßige Berichterstattung, laufende Überwachung, Besuche vor Ort oder Stichprobenprüfungen erreicht werden;

    b) Durchführung von Bewertungen, um sicherzustellen, dass der externe Dienstleister ausreichend ausgestattet und in der Lage ist, das Verfahren zum Fern-Kundenannahmeprozess durchzuführen. Die Bewertungen können unter anderem eine Beurteilung der Schulung des Personals, der technologischen Eignung und der Daten-Governance des externen Dienstleisters umfassen;

    c) Sicherstellung, dass der externe Dienstleister die Kredit- und Finanzinstitute über alle vorgeschlagenen Änderungen des Verfahrens zum Fern-Kundenannahmeprozess

[8] EBA/GL/2021/02.

[9] EBA-Leitlinien zu Auslagerungen.docx (europa.eu).

oder jede Änderung der vom externen Dienstleister bereitgestellten Anwendung informiert.

49. Wenn der externe Dienstleister während des Verfahrens zum Fern-Kundenannahmeprozess Kundendaten, darunter Fotos, Videos und Dokumente, speichert, sollten die Kredit- und Finanzinstitute sicherstellen, dass

    a) nur die erforderlichen Kundendaten im Einklang mit einer klar definierten Speicherfrist erhoben und gespeichert werden;

    b) der Zugang zu den Daten streng begrenzt ist und registriert wird;

    c) geeignete Sicherheitsmaßnahmen getroffen werden, um den Schutz der gespeicherten Daten zu gewährleisten.

4.6 Management von IKT- und Sicherheitsrisiken

50. Die Kredit- und Finanzinstitute sollten ihre IKT- und Sicherheitsrisiken im Zusammenhang mit der Nutzung des Verfahrens zum Fern-Kundenannahmeprozess ermitteln und steuern, auch wenn die Kredit- und Finanzinstitute auf Dritte zurückgreifen oder die Dienstleistung ausgelagert wird, einschließlich der Auslagerung an Unternehmen der eigenen Gruppe.

51. Zusätzlich zur Erfüllung der Anforderungen der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken[10], sofern zutreffend, sollten die Kredit- und Finanzinstitute während des Verfahrens zum Fern-Kundenannahmeprozess sichere Kommunikationskanäle für die Interaktion mit dem Kunden nutzen. Zur Wahrung der Vertraulichkeit, Authentizität und Integrität der ausgetauschten Daten sollte sich die Anwendung für den Fern-Kundenannahmeprozess gegebenenfalls auf sichere Protokolle und kryptografische Algorithmen im Einklang mit den bewährten Verfahren der Branche stützen.

52. Die Kredit- und Finanzinstitute sollten einen sicheren Zugangspunkt für den Beginn des Verfahrens zum Fern-Kundenannahmeprozess bereitstellen, der auf qualifizierten Zertifikaten für elektronische Siegel nach Artikel 3 Absatz 30 der Verordnung (EU) Nr. 910/2014 oder für die Website-Authentifizierung nach Artikel 3 Absatz 39 der genannten Verordnung basiert. Zudem sollte der Kunde über die anwendbaren Sicherheitsmaßnahmen informiert werden, die ergriffen werden sollten, um eine sichere Nutzung des Systems zu gewährleisten.

53. Wenn ein Mehrzweckgerät für die Durchführung des Verfahrens zum Fern-Kundenannahmeprozess eingesetzt wird, sollte gegebenenfalls eine sichere Umgebung für die Ausführung des Softwarecodes auf der Kundenseite verwendet werden. Es sollten zusätzliche Sicherheitsmaßnahmen ergriffen werden, um die Sicherheit und Zuverlässigkeit des Softwarecodes und der erhobenen Daten gemäß der Sicherheitsrisikobewertung im

[10] EBA/GL/2019/04.

Einklang mit den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken zu gewährleisten.

4.7 Einhaltung dieser Leitlinien, wenn die Kredit- und Finanzinstitute Vertrauensdienste und nationale Verfahren zur Feststellung der Identität gemäß Artikel 13 Absatz 1 Buchstabe a der Richtlinie (EU) 2015/849 nutzen

54. Die Kredit- und Finanzinstitute können zur Erfüllung dieser Leitlinien einschlägige Vertrauensdienste und elektronische Verfahren zur Feststellung der Identität nutzen, die von den zuständigen nationalen Behörden gemäß Artikel 13 Absatz 1 Buchstabe a der Richtlinie (EU) 2015/849 reguliert, anerkannt, genehmigt oder akzeptiert werden. Bei der Nutzung dieser Anwendungen sollten die Kredit- und Finanzinstitute bewerten, inwieweit die Anwendung den Bestimmungen dieser Leitlinien entspricht, und die erforderlichen Maßnahmen ergreifen, um alle relevanten Risiken, die sich aus der Nutzung dieser Anwendungen ergeben, zu mindern. Dabei sollte insbesondere berücksichtigt werden, ob den folgenden Risiken Rechnung getragen wird:

    a) die mit der Authentifizierung verbundenen Risiken und die in ihren Strategien und Verfahren festgelegten spezifischen Maßnahmen zur Risikominderung, insbesondere hinsichtlich Risiken der Identitätserschleichung;

    b) das Risiko, dass die Identität des Kunden nicht mit der angegebenen Identität übereinstimmt;

    c) das Risiko verloren gegangener, gestohlener, ausgesetzter, widerrufener oder abgelaufener Identitätsnachweise, gegebenenfalls einschließlich Instrumente zur Aufdeckung und Verhinderung von Identitätsbetrug.