EBA/GL/2024/11

4. Juli 2024

Leitlinien

Leitlinien zu Informationspflichten in Bezug auf Geldtransfers und Transfers bestimmter Kryptowerte gemäß der Verordnung (EU) 2023/1113 (im Folgenden „Leitlinien zur Transferregelung“)

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 herausgegeben wurden. [1] 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 die für sie geltenden Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken integrieren (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren), und zwar einschließlich der Leitlinien, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 27.11.2024 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständigen Behörden den Anforderungen nicht nachkommen. Die Meldungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2024/11“ zu übermitteln. Die Meldungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer zuständigen Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

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

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

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

5. Mit diesen Leitlinien wird das Mandat zur Herausgabe von Leitlinien gemäß Artikel 36 Unterabsätze 1 und 2 der Verordnung (EU) 2023/1113 erfüllt[2].

6. Diese Leitlinien legen insbesondere Folgendes fest:

   a) beschreiben die Faktoren, die Zahlungdienstleister (PSP), zwischengeschaltete Zahlungdienstleister (IPSP), Anbieter von Krypto-Dienstleistungen (CASP) und zwischengeschaltete Anbieter von Krypto-Dienstleistungen (ICASP) berücksichtigen sollten, wenn sie Verfahren zur Feststellung und Bearbeitung von Geldtransfers und Kryptowerten einrichten, bei denen die vorgeschriebenen Angaben zum Zahler/Originator bzw. zum Zahlungsempfänger/Begünstigten fehlen, und um sicherzustellen, dass diese Verfahren wirksam sind;

   b) geben im Einzelnen vor, wie PSP, CASP, IPSP und ICASP das Risiko der Geldwäsche (GW) oder Terrorismusfinanzierung (TF) mindern sollten, wenn vorgeschriebene Angaben zum Zahler, Originator, Zahlungsempfänger oder Begünstigten fehlen oder unvollständig sind;

   c) präzisieren die technischen Aspekte der Anwendung der Verordnung (EU) 2023/1113 in Bezug auf Lastschriften.

7. Darüber hinaus erfüllen diese Leitlinien das Mandat, Leitlinien gemäß Artikel 19a Absatz 2 der Richtlinie (EU) 2015/849 [3] herauszugeben, in denen Maßnahmen zur Ermittlung und Beurteilung der Risiken von Geldwäsche und Terrorismusfinanzierung im Zusammenhang mit Kryptowertetransfers, welche an eine selbst gehostete Adresse gerichtet sind oder von ihr ausgehen, festgelegt werden.

[2] Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 (ABl. L 150 vom 9.6.2023, S. 1).

[3] 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, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. L 141 vom 5.6.2015, S. 73).

Adressaten

8. Die vorliegenden Leitlinien richten sich an:

   a) PSP im Sinne des Artikels 3 Nummer 5 der Verordnung (EU) 2023/1113 und IPSP im Sinne des Artikels 3 Nummer 6 der Verordnung (EU) 2023/1113;

   b) CASP gemäß der Definition in Artikel 3 Nummer 15 der Verordnung (EU) 2023/1113 und ICASP gemäß der Definition in Artikel 3 Nummer 16 der Verordnung (EU) 2023/1113;

   c) zuständige Behörden, die überwachen, ob PSP, IPSP, CASP und ICASP den ihnen aus der Verordnung (EU) 2015/847 erwachsenden Pflichten nachkommen.

Begriffsbestimmungen

9. Sofern nicht anders angegeben, haben die in der Verordnung (EU) 2023/1113, in der Richtlinie (EU) 2015/849 und der Richtlinie (EU) 2015/2366 verwendeten und definierten Begriffe in den Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

Risiko	bezeichnet die Wahrscheinlichkeit für Geldwäsche und Terrorismusfinanzierung und die damit verbundenen Auswirkungen.
Risikofaktoren	bezeichnet Variablen, die entweder für sich allein genommen oder in Kombination miteinander das GW/TF-Risiko einer einzelnen Geschäftsbeziehung oder einer gelegentlichen Transaktion oder eines gelegentlichen Transfers erhöhen oder verringern können.
Risikobasierter Ansatz	bezeichnet einen Ansatz, nach dem die zuständigen Behörden und PSP, IPSP, CASP und ICASP die Risiken für Geldwäsche und Terrorismusfinanzierung, denen die PSP, IPSP, CASP und ICASP ausgesetzt sind, ermitteln, bewerten und verstehen sowie Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung ergreifen, die diesen Risiken angemessen sind.
Transferkette	bezeichnet die durchgängige Abfolge von Parteien, Prozessen und Interaktionen, die an der Ermöglichung des Geldtransfers und des Kryptowertetransfers gemäß der Verordnung (EU) Nr. 2023/1113 vom Zahler oder Originator an den Zahlungsempfänger oder Begünstigten beteiligt sind.

3. Umsetzung

Geltungsbeginn

10. Diese Leitlinien gelten ab dem 30. Dezember 2024.

Aufhebung

11. Die „Gemeinsamen Leitlinien nach Artikel 25 der Verordnung (EU) 2015/847 zu den Maßnahmen, mit deren Hilfe Zahlungsdienstleister das Fehlen oder die Unvollständigkeit von Angaben zum Zahler und zum Begünstigten feststellen können, und zu den empfohlenen Verfahren für die Bearbeitung eines Geldtransfers, bei dem die vorgeschriebenen Angaben fehlen“[4] werden zum 30. Dezember 2024 aufgehoben.

[4] JC/GL/2017/16

4. Informationspflichten in Bezug auf Geldtransfers und Transfers bestimmter Kryptowerte gemäß der Verordnung (EU) 2023/1113

4.1. Allgemeine Bestimmungen

Geldtransfers und Kryptowertetransfer

12. Um festzulegen, welche Angaben einem Geldtransfer oder einem Kryptowertetransfer beizufügen sind und welche Schritte sie unternehmen sollten, um die Verordnung (EU) 2023/1113 einzuhalten, sollten PSP, IPSP, CASP und ICASP in ihren Strategien und Verfahren festlegen, wie sie bei jedem Geldtransfer oder Transfer von Kryptowerten feststellen, ob sie handeln als:

    a) der PSP des Zahlers, des Zahlungsempfängers oder ein IPSP;

    b) der CASP des Originators, des Begünstigten oder ein ICASP.

13. PSP, IPSP, CASP und ICASP sollten sicherstellen, dass die Strategien und Verfahren, die sie zur Einhaltung von Artikel 7 Absätze 1 und 2, Artikel 8 Absatz 1, Artikel 11 Absätze 1 und 2, Artikel 12 Absatz 1, Artikel 16 Absatz 1, Artikel 17 Absatz 1, Artikel 20 und Artikel 21 Absatz 1 der Verordnung (EU) Nr. 2023/1113 eingeführt haben, wirksam sind und bleiben, indem sie beispielsweise Kontrollen einer beliebigen Stichprobe aus allen ausgeführten Transfers vornehmen.

14. PSP, IPSP, CASP und ICASP sollten ihre Strategien und Verfahren auf dem neuesten Stand halten und sie bei Bedarf verbessern.

4.2. Ausnahmen vom Anwendungsbereich der Verordnung (EU) 2023/1113 und Abweichungen

Geldtransfers und Kryptowertetransfer

15. PSP und CASP sollten in ihren Strategien und Verfahren darlegen, wie sie feststellen, ob die Bedingungen für die Anwendung der in Artikel 2 der Verordnung (EU) 2023/1113 genannten Ausnahmen oder Abweichungen erfüllt sind. PSP und CASP, die nicht feststellen können, ob die Voraussetzungen erfüllt sind, sollten bei allen Geldtransfers und Kryptowertetransfers die Vorschriften der Verordnung (EU) 2023/1113 einhalten.

4.2.1. Feststellung, ob eine Karte, ein Instrument oder ein Gerät ausschließlich zur Bezahlung von Waren oder Dienstleistungen im Sinne von Artikel 2 Absatz 3 Buchstabe a und Absatz 5 Buchstabe b der Verordnung (EU) 2023/1113 verwendet wird

Geldtransfers und Kryptowertetransfer

16. PSP und CASP sollten einen Geldtransfer oder Kryptowertetransfer als Zahlung für Waren oder Dienstleistungen behandeln, wenn der Transfer von einem Kunden (Käufer) an einen Händler (Verkäufer) im Austausch für den Kauf von Waren oder die Erbringung von Dienstleistungen erfolgt. Um festzustellen, ob eine Karte, ein Instrument oder ein Gerät ausschließlich zur Bezahlung von Waren oder Dienstleistungen verwendet wird, sollten PSP und CASP nachweisen, dass mindestens eine der folgenden Bedingungen erfüllt ist:

    a) ob die Funktionalität der verwendeten Karte, des Instruments oder des Geräts auf die Bezahlung von Waren oder Dienstleistungen beschränkt ist;

    b) ob den Kunden ein Händlerkategorisierungscode zugewiesen wird, einschließlich des Händlerkategorisierungscodes (MCC) von Zahlungskartensystemen, der zur Kategorisierung der Art der verkauften Waren oder Dienstleistungen verwendet wird;

    c) ob der Kunde eine wirtschaftliche oder berufliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, unter Verwendung von Informationen, die für die Zwecke von Artikel 13 der Richtlinie (EU) 2015/849 erhoben wurden, falls verfügbar, oder von Informationen, die über Drittanbieter oder in öffentlich zugänglichen Quellen zugänglich sind; und

    d) ob anhand der vom PSP oder CASP vorgenommenen Analyse von Trends und Verhaltensweisen, einschließlich Transferhistorien und -mustern, feststellt werden kann, ob Zahler und Originator Zahlungen für Waren oder Dienstleistungen tätigen oder Zahlungsempfänger und Begünstigter Zahlungen für Waren oder Dienstleistungen erhalten.

4.2.2. Verbundene Transfers in Bezug auf den Schwellenwert von 1 000 EUR gemäß Artikel 2 Absatz 5 Buchstabe c, Artikel 5 Absatz 2, Artikel 6 Absatz 2 und Artikel 7 Absatz 3 der Verordnung (EU) 2023/1113

Geldtransfers

17. PSP sollten über Strategien und Verfahren verfügen, um Transfers zu erkennen, die scheinbar miteinander verbunden sind.

18. PSP sollten Transfers als miteinander verbunden behandeln, die:

    a) in einem einzigen Vorgang oder in mehreren Transaktionen durchgeführt werden und

b) von ein und demselben Zahler an ein und denselben Zahlungsempfänger innerhalb eines kurzen Zeitraums gesendet werden; oder

c) die innerhalb eines kurzen Zeitraums von einem Zahler an verschiedene Zahlungsempfänger oder von verschiedenen Zahlern an denselben Zahlungsempfänger gesendet werden; dazu gehören auch Fälle, in denen verschiedene Konten derselben Person verwendet werden oder verschiedene Transaktionen für dieselbe Person getätigt werden, sofern diese Angaben dem PSP bekannt sind.

19. PSP sollten in ihren Strategien und Verfahren Folgendes klar darlegen:

a) was ein kurzer Zeitrahmen für verschiedene Arten von Transfers ist; die PSP sollten diesen Zeitrahmen in einer Weise festlegen, die dem GW-/TF-Risiko, dem ihre Geschäfte ausgesetzt sind, angemessen ist, und zwar auf der Grundlage der Risikobewertungen, die sie im Einklang mit den Leitlinien der EBA zu Risikofaktoren für Geldwäsche und Terrorismusfinanzierung durchgeführt haben[5];

b) wie sie Versuche ermitteln, den Schwellenwert zu umgehen oder sich der Aufdeckung zu entziehen, und

c) alle anderen Szenarien, die ebenfalls zu verbundenen Transaktionen führen könnten.

20. PSP sollten, bestimmen, ob ein Transfer zum Zeitpunkt, zu dem der Transfer angeordnet oder eingeleitet wurde, verbunden ist. Dabei sollte der zu transferierenden Betrag nach Abzug von Gebühren, die vom PSP erhoben werden, zugrunde gelegt werden.

4.3. Übermittlung und Erhalt von Angaben im Rahmen des Transfers gemäß den Artikeln 4 bis 8, 10 bis 12, 14 bis 17 und 19 bis 21 der Verordnung (EU) 2023/1113

4.3.1. Nachrichten- oder Zahlungs- und Abwicklungssysteme

Geldtransfers und Kryptowertetransfers

21. PSP, IPSP, CASP und ICASP sollten Infrastrukturen und Dienste für die Übermittlung und den Erhalt von Angaben nutzen, die technisch in der Lage sind, die Angaben vollständig und ohne Auslassungen oder Fehler in der Darstellung der Angaben gemäß diesen Leitlinien zu übermitteln und zu erhalten.

22. PSP, IPSP, CASP und ICASP sollten sicherstellen, dass ihre Systeme in der Lage sind, die Datenintegrität aufrechtzuerhalten, insbesondere, wenn Angaben vor dem Transfer oder nach dem Erhalt in ein anderes Format umgewandelt werden müssen. PSP, IPSP, CASP und ICASP, die nicht gewährleisten können, dass ihre Systeme die Angaben ohne Fehler oder Auslassungen

[5] EBA/CP/2023/11.

übermitteln, erhalten oder umwandeln können, sollten zu einem System wechseln, das dazu in der Lage ist.

23. PSP, IPSP, CASP und ICASP sollten sicherstellen, dass die Systeme, die sie für die Übermittlung von Angaben verwenden, sicher sind. Die CASP sollten auch die Hinweise anwenden, die den PSP in den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken[6] und den EBA-Leitlinien zu Auslagerungsvereinbarungen zur Verfügung gestellt werden[7].

Kryptowertetransfers

24. Abweichend von Absatz 21 können CASP und ICASP bis zum 31. Juli 2025 ausnahmsweise Infrastrukturen oder Dienste nutzen, bei denen technische Einschränkungen in Bezug auf die Vollständigkeit der Daten durch zusätzliche technische Schritte oder Korrekturen ausgeglichen werden müssen, um diesen Leitlinien vollständig zu entsprechen. Diese zusätzlichen Verfahren sollten zumindest alternative Mechanismen für die Erfassung, Aufbewahrung und Bereitstellung der Angaben, die aufgrund technischer Einschränkungen nicht übermittelt werden können, für den erhaltenden CASP oder ICASP in der Transferkette umfassen.

25. Bei der Übermittlung von Angaben gemäß Artikel 14 der Verordnung (EU) 2023/1113 sollten der CASP des Originators und der ICASP:

    a) die Angaben entweder als Teil des Transfers auf der Blockchain oder auf einer anderen Distributed-Ledger-Technologie (DLT)-Plattform oder unabhängig davon über verschiedene Kommunikationskanäle übermitteln - einschließlich der direkten Kommunikation zwischen CASP, Anwendungsprogrammierschnittstellen (API), Code-Lösungen, die auf der Blockchain laufen, und anderen Lösungen von Drittanbietern; und

    b) die vorgeschriebenen Angaben sofort und sicher übermitteln, und zwar spätestens bei der Ausführung der Blockchain-Transaktion.

26. Bei der Auswahl des Nachrichten- oder Zahlungs- und Abwicklungssystems/der Nachrichten- oder Zahlungs- und Abwicklungssysteme sollten CASP und ICASP verhältnismäßige, risikosensitive Maßnahmen ergreifen, um Folgendes zu bewerten:

    a) die Fähigkeit des Systems, mit anderen internen zentralen Systemen sowie mit den Nachrichten- oder Zahlungs- und Abwicklungssystemen der Gegenpartei eines Transfers zu kommunizieren, und seine Kompatibilität mit anderen Blockchain-Netzwerken;

[6] EBA/GL/2019/04.

[7] EBA/GL/2019/02.

b) die Erreichbarkeit des Protokolls (d. h. die Vielfalt und Genauigkeit der Gegenparteien, die mit dem Protokoll erreicht werden können – vorbehaltlich der eigenen Due-Diligence-Bewertung des CASP – und die Quote der Transfers, die erfolgreich an den vorgesehenen Begünstigten gesendet oder vom Originator erhalten wurden);

c) wie das System es dem CASP oder dem ICASP ermöglicht, einen Transfer mit fehlenden oder unvollständigen Angaben zu erkennen;

d) die Kapazitäten für die Datenintegration, Datensicherheit und -zuverlässigkeit des Systems.

4.3.2. Multi-Intermediation und grenzüberschreitende Transfers

Geldtransfers

27. PSP und IPSP, die die Ausführung von Transfers mit zwei oder mehr IPSP oder PSP auf grenzüberschreitender Basis ermöglichen, sollten in ihren Strategien und Verfahren beschreiben, wie die Angaben über den Zahler und den Zahlungsempfänger über die gesamte Transferkette hinweg an den nächsten PSP und IPSP in der Transferkette übermittelt werden.

28. Bei Transfers, die nicht verbunden wurden, sollte der PSP oder der IPSP:

a) die Transferkette (von einem Ende zum anderen) als eine solche betrachten, bei der der Informationsfluss über den ursprünglichen Zahler und den Zahlungsempfänger erhalten bleibt;

b) wenn der Transfer von einem grenzüberschreitenden auf einen inländischen Kanal erfolgt, das nationale System auswählen, das die Transparenz des grenzüberschreitenden Charakters des Transfers maximiert und sicherstellt, dass die Angaben über die Parteien, die an den nächsten PSP in der Zahlungskette übermittelt werden, von allen zwischengeschalteten und/oder begünstigten PSP leicht verstanden werden können;

c) in Zweifelsfällen davon ausgehen, dass es sich um einen grenzüberschreitenden Transfer handelt, was die Nutzung geeigneter Zahlungswege zur Folge hat, die die erforderliche Übermittlung von Angaben erleichtern können.

29. PSP sind – vorbehaltlich der in den Artikeln 10 bis 13 der Verordnung (EU) 2023/1113 vorgeschriebenen spezifischen Kontrolle – nur für die Weiterleitung der Zahlungsnachricht unter Verwendung der Daten verantwortlich, die ihnen vom vorangehenden PSP/IPSP in der Transferkette übermittelt wurden.

30. PSP und IPSP sollten einen Transfer vom Zahler zum Zahlungsempfänger nicht als Liquiditätsbewegung oder -abwicklung auf eigene Rechnung des PSP und des IPSP behandeln.

Geldtransfers und Kryptowertetransfers

31. Erhält der Intermediär nicht die vorgeschriebenen Angaben im Zusammenhang mit einem Transfer, insbesondere im Falle von verbundenen Transfers, sollten der IPSP oder ICASP die fehlenden Angaben über einen alternativen Kanal-Mechanismus, einschließlich Methoden wie API und Drittanbieter-Lösungen, einholen, um die Anforderungen der Verordnung (EU) 2023/1113 zu erfüllen.

4.4. Beim Transfer gemäß den Artikeln 4 und 14 der Verordnung (EU) 2023/1113 zu übermittelnde Angaben

Geldtransfers und Kryptowertetransfers

32. PSP und CASP sollten die ursprüngliche Übermittlung nicht ändern, es sei denn:

    a) sie werden von dem IPSP, dem PSP des Zahlungsempfängers, dem ICASP oder dem CASP des Begünstigten dazu aufgefordert, wenn die IPSP, der PSP des Zahlungsempfängers, der ICASP oder der CASP des Begünstigten der Ansicht sind, dass einige der Angaben gemäß den Artikeln 7, 11, 19 oder 20 der Verordnung (EU) 2023/1113 fehlen; oder

    b) der PSP des Zahlers oder der CASP des Originators stellt nach dem Transfer einen Fehler in den Angaben fest, die sie zur Einhaltung der Artikel 4 und 14 der Verordnung (EU) 2023/1113 übermittelt haben.

33. Kommt es im Zusammenhang mit Absatz 32 zu einer Änderung der ursprünglichen Übermittlung, sollte der PSP des Zahlers oder der CASP des Originators den nächsten PSP und CASP in der Transferkette informieren und die korrekten Angaben übermitteln. Der nächste PSP und der nächste CASP in der Transferkette sollten dann erneut die notwendigen Aufgaben wahrnehmen, um die fehlenden oder unvollständigen Angaben zu erkennen.

4.4.1. Angabe der Nummer des Zahlungskontos des Zahlers gemäß Artikel 4 Absatz 1 Buchstabe b der Verordnung (EU) 2023/1113 und des Zahlungsempfängers (Artikel 4 Absatz 2 Buchstabe b der Verordnung (EU) 2023/1113)

Geldtransfers

34. PSP sollten sicherstellen, dass im Zuge des Geldtransfers die Nummer des Zahlungskontos angegeben wird. Erfolgt der Geldtransfer mit einer Zahlungskarte, so kann die Nummer dieser Karte (Stammkontonummer – Primary Account Number [PAN]) an die Stelle der Nummer des Zahlungskontos treten, sofern diese Nummer es ermöglicht, den Geldtransfer zum Zahler oder zum Zahlungsempfänger zurückzuverfolgen.

4.4.2. Angabe des Namens des Zahlers, des Zahlungsempfängers, des Originators und des Begünstigten gemäß Artikel 4 Absatz 1 Buchstabe a, Artikel 4 Absatz 2 Buchstabe a, Artikel 14 Absatz 1 Buchstabe a und Artikel 14 Absatz 2 Buchstabe a der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

35. Der PSP des Zahlers oder der CASP des Originators sollte folgende Angaben machen:

a) Bei natürlichen Personen die vollständigen Vor- und Nachnamen des Kunden, wie sie im Ausweisdokument des Kunden oder im elektronischen Identitätsnachweis, der den Standards in Artikel 13 der Richtlinie (EU) 2015/849 entspricht, aufgeführt sind, oder, falls beides aus berechtigten Gründen nicht verfügbar ist, die Dokumentation gemäß den EBA-Leitlinien zu Strategien und Kontrollen für die wirksame Steuerung von Risiken für Geldwäsche und Terrorismusfinanzierung (GW/TF) bei der Bereitstellung eines Zugangs zu Finanzdienstleistungen[8]. Bestehen technische Beschränkungen gemäß Absatz 24, die eine Übermittlung der Namen und Nachnamen des Kunden verhindern, sollte der CASP des Originators mindestens den ersten Vornamen und den letzten Nachnamen enthalten.

b) Bei juristischen Personen der Name, unter dem die juristische Person eingetragen ist. Bestehen technische Beschränkungen gemäß Absatz 24, die die Übermittlung des vollständigen eingetragenen rechtlichen Namens verhindern, sollte der CASP des Originators den Handelsnamen übermitteln. Die verwendeten Handelsnamen sollten eindeutig auf die juristische Person zurückverfolgt werden können und mit diesen in amtlichen Registern eingetragenen Namen übereinstimmen.

c) Bei Transfers von einem gemeinsamen Konto, einer gemeinsamen Adresse oder einer gemeinsamen Wallets die Namen aller Inhaber des Kontos, der Adresse oder des Wallets. Bestehen technische Beschränkungen gemäß Absatz 24, die die Übermittlung aller Namen aller an dem Transfer beteiligten Parteien verhindern, sollte der CASP des Originators den Namen des Inhabers des Kontos, der Adresse oder des Wallets, der den Transfer veranlasst, oder, falls dies nicht möglich ist, den Namen des Inhabers des Stammkontos, der Adresse oder des Wallets angeben.

4.4.3. Angabe der Anschrift des Zahlers und des Originators, einschließlich der Angabe des Landes, der Nummer des amtlichen persönlichen Dokuments und der Kundennummer oder alternativ des Geburtsdatums und -orts des Zahlers gemäß Artikel 4 Absatz 1 Buchstabe c und Artikel 14 Absatz 1 Buchstabe d der Verordnung (EU) 2023/1113

[8] EBA/GL/2023/04.

Geldtransfers und Kryptowertetransfers

36. Der PSP des Zahlers und der CASP des Originators sollten Folgendes angeben:

    a) Bei natürlichen Personen den gewöhnlichen Wohnsitz des Zahlers oder Originators oder, wenn es keine feste Wohnanschrift gibt, die Postanschrift, unter der die natürliche Person erreicht werden kann. Im Falle einer gefährdeten Person im Sinne von Absatz 19 Buchstabe b der EBA-Leitlinien zu Strategien und Kontrollen für die wirksame Steuerung von Risiken für Geldwäsche und Terrorismusfinanzierung (GW/TF) bei der Bereitstellung eines Zugangs zu Finanzdienstleistungen, von denen vernünftigerweise nicht erwartet werden kann, dass sie eine Adresse in Bezug auf ihren üblichen Wohnsitz angeben, kann der PSP oder der CASP eine Anschrift verwenden, die in alternativen Unterlagen gemäß Absatz 19 Buchstabe b der oben genannten Leitlinien angegeben ist, sofern diese Unterlagen eine Anschrift enthalten und ihre Verwendung nach dem nationalen Recht des Zahlers zulässig ist.

    b) Bei juristischen Personen die registrierte Anschrift des Zahlers oder Originators oder des offiziellen Sitzes des Zahlers oder Originators.

37. Die Anschrift sollte, soweit möglich, in folgender Rangfolge angegeben werden: vollständiger Ländername oder Abkürzung gemäß dem Internationalen Standard für Ländercodes (ISO 3166) (Alpha-2 oder Alpha-3), Postleitzahl, Stadt, Staat und Provinz und Gemeinde, Straßenname, Gebäudenummer oder Gebäudename.

38. Der PSP des Zahlers und der CASP des Originators sollten die in Absatz 37 genannte Postanschrift angeben. Unbeschadet des Absatzes 25 Buchstabe a sollte bei allen alternativen zu Postanschriften, einschließlich Postfachnummern und virtuellen Adressen, nicht davon ausgegangen werden, dass sie die Anforderungen nach Artikel 4 Absatz 1 Buchstabe c und Artikel 14 Absatz 1 Buchstabe d der Verordnung (EU) 2023/1113 erfüllen.

39. Die Kombination der gemäß Artikel 4 Absatz 1 Buchstabe c und Artikel 14 Absatz 1 Buchstabe d der Verordnung (EU) 2023/1113 bereitzustellenden alternativen Angaben sollten nicht nur darauf beruhen, ob sie verfügbar sind, sondern auch darauf, welche Angaben am besten eine eindeutige Identifizierung des Zahlers oder Originators ermöglichen.

40. Bei Transfers von einem gemeinsamen Konto, einer gemeinsamen Adresse oder einem gemeinsamen Wallet sollten die Angaben zu allen Inhabern des Kontos, der Adresse oder des Wallets bereitgestellt werden. Kann die Übermittlung der jeweiligen Angaben aller Parteien aufgrund technischer Einschränkungen gemäß Absatz 24 nicht erfolgen, so sollten der PSP des Zahlers und der CASP des Originators die Angaben zum Inhaber des Kontos, der Adresse oder des Wallets, der den Transfer veranlasst, oder alternativ zum Inhaber des Stammkontos, der Adresse oder des Wallets übermitteln.

4.4.4. Angabe einer gleichwertigen Kennung zur Rechtsträgerkennung („legal entity identifier“, im Folgenden „LEI“) des Zahlers, des Zahlungsempfängers, des Originators und des Begünstigten gemäß Artikel 4 Absatz 1 Buchstabe d, Artikel 4 Absatz 2 Buchstabe c, Artikel 14 Absatz 1 Buchstabe e und Artikel 14 Absatz 2 Buchstabe d der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

41. Der PSP des Zahlers und der CASP des Originators sollten nur solche amtlichen Kennungen als gleichwertig mit einer LEI betrachten, die:

    a) aus einem einzigen Identifikationscode bestehen, der für die juristische Person einzigartig ist;

    b) in öffentlichen Registern veröffentlicht werden;

    c) bei Gründung eines Unternehmens durch eine Behörde in dem Land ausgestellt werden, in dem die juristische Person ihren Sitz hat.

    d) die Identifizierung der Namens- und Adressbestandteile ermöglichen; und

    e) eine Beschreibung der Art der im Nachrichtensystem verwendeten Kennung enthalten.

4.5. Feststellung fehlender Angaben gemäß den Artikeln 7, 11, 16 und 20 der Verordnung (EU) 2023/1113

4.5.1. Verfahren zur Erkennung fehlender Angaben gemäß den Artikeln 7, 11, 16 und 20 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

42. Die in den Artikeln 7, 11, 16 und 20 der Verordnung (EU) 2023/1113 genannten Verfahren sollten mindestens Folgendes umfassen:

    a) die Schritte zur Erkennung von fehlenden, unvollständigen und bedeutungslosen Angaben oder unzulässigen Buchstaben oder Einträgen;

    b) eine Kombination von Überwachungspraktiken während und nach dem Transfer, die dem Ausmaß des GW-/TF-Risikos, dem die Transfers ausgesetzt sind, angemessen ist und gemäß den Leitlinien der EBA zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung bestimmt wird; und

    c) die Kriterien, die PSP, IPSP, CASP und ICASP bei der Erkennung risikoerhöhender Faktoren helfen, wie in Absatz 52 beschrieben.

4.5.2. Kontrollen der zulässigen Buchstaben und Einträge bei Geldtransfers gemäß Artikel 7 Absatz 1 und Artikel 11 Absatz 1 der Verordnung (EU) 2023/1113

Geldtransfers

43. PSP und IPSP der Zahlungsempfänger sollten in Bezug auf ihre Nachrichten- oder Zahlungs- und Abwicklungssysteme sicherstellen, dass:

    a) sie die Validierungsregeln des Systems verstehen;

    b) das System alle Felder enthält, die erforderlich sind, um die in der Verordnung (EU) 2023/1113 geforderten Angaben einzugeben, wie in Abschnitt 4.4. beschrieben;

    c) das System das Senden oder den Erhalt von Transfers automatisch verhindert, wenn unzulässige Buchstaben oder Einträge erkannt werden; und

    d) das System zurückgewiesene Transfers zur manuellen Überprüfung und Bearbeitung kennzeichnet.

44. Wenn das Nachrichten- oder Zahlungs- und Abwicklungssystem eines PSP oder IPSP nicht alle in Absatz 43 aufgeführten Kriterien erfüllt, sollte der betreffende PSP oder IPSP Kontrollen einführen, um diese Mängel zu mitigieren.

45. PSP des Zahlers und IPSP sollten in ihren Strategien und Verfahren Folgendes festlegen:

    a) wie sie feststellen, ob die Felder, die sich auf die Angaben im Nachrichten- oder Zahlungs- und Abwicklungssystem beziehen, mit Buchstaben oder Einträgen ausgefüllt wurden, die den im Einklang mit den Regeln des betreffenden Systems stehen; und

    b) die Schritte, die sie unternehmen werden, wenn die Buchstaben oder Einträge nicht den im Einklang mit den Regeln des betreffenden Systems stehen.

4.5.3. Überwachung von Transfers gemäß Artikel 7 Absatz 2, Artikel 11 Absatz 2, Artikel 16 Absatz 1 und Artikel 20 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

46. PSP des Zahlungsempfängers, IPSP, CASP des Begünstigten oder ICASP sollten in ihren Strategien und Verfahren festlegen, wie sie bestimmen, welche Transfers während oder nach der Überweisung gemäß Artikel 7 Absatz 2, Artikel 11 Absatz 2, Artikel 16 Absatz 1 und Artikel 20 der Verordnung (EU) 2023/1113 überwacht werden. PSP, IPSP, CASP und ICASP sollten mindestens Folgendes festlegen:

    a) welche Risikofaktoren sie bei dieser Bewertung berücksichtigen werden; und

    b) welche risikoerhöhenden Faktoren oder Kombinationen von risikoerhöhenden Faktoren immer eine Überwachung während des Transfers und welche eine gezielte Überprüfung nach dem Transfer auslösen.

47. PSP, IPSP, CASP und ICASP sollten die Risikofaktoren auf der Grundlage der in den Leitlinien der EBA für GW/TF-Risikofaktoren festgelegten Risikofaktoren sowie die relevanten Risikofaktoren aus ihrer unternehmensweiten und der sektorspezifischen oder nationalen Risikobewertung, soweit diese verfügbar ist, bestimmen. Zu den Risikofaktoren sollten mindestens folgende gehören:

    a) Transfers, die einen vorher festgelegten Schwellenwert überschreiten, unter Berücksichtigung des Durchschnittswerts der von ihnen routinemäßig bearbeiteten Transfers und dessen, was einen ungewöhnlich großen Transfer darstellt, basierend auf ihrem jeweiligen Geschäftsmodell;

    b) Transfers, bei denen der Zahler, der Originator, der Zahlungsempfänger, der Begünstigte, der PSP des Zahlers, der CASP des Originators, der PSP des Zahlungsempfängers oder der CASP des Begünstigten in Ländern oder Gebieten ansässig sind, die restriktiven Maßnahmen, einschließlich gezielter finanzieller Sanktionen, unterliegen, oder in Ländern oder Gebieten, in denen ein hohes Risiko der Umgehung restriktiver Maßnahmen oder gezielter finanzieller Sanktionen besteht;

    c) Transfers, bei denen Zahler, Originator, Zahlungsempfänger, Begünstigter, PSP des Zahlers, CASP des Originators, PSP des Zahlungsempfängers oder der CASP des Begünstigten in einem Land ansässig sind, das mit einem hohen GW-/TF-Risiko verbunden ist, einschließlich, aber nicht nur:

        i) Länder, die von der Europäischen Kommission gemäß Artikel 9 der Richtlinie (EU) 2015/849 als Länder mit hohem Risiko eingestuft wurden; und

        ii) Länder, in denen auf der Grundlage glaubwürdiger Quellen wie Bewertungen, gegenseitige Evaluierungen, Bewertungsberichte oder veröffentlichte Follow-up-Berichte Anforderungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung bestehen, die nicht im Einklang mit der Richtlinie (EU) 2015/849 oder den FATF-Empfehlungen stehen, und Länder, die diese Anforderungen nicht wirksam umgesetzt haben;

    d) Transfers, bei denen der PSP des Zahlers, der CASP des Originators, der IPSP, der ICASP und der PSP des Zahlungsempfängers oder der CASP des Begünstigten in einem Land ansässig sind, das nach öffentlich zugänglichen Angaben die Verpflichtung zur Einholung, Aufbewahrung und Übermittlung von Angaben über den Originator und den Begünstigten bei der Durchführung von Geldtransfers und virtuellen Transfers von virtuellen Vermögenswerten noch nicht umgesetzt hat;

    e) Transfers mit Unternehmen, die in einem Drittland ansässig sind, das keine Zulassungsregelungen hat oder die Tätigkeit von PSP im Falle von Geldtransfers und CASP im Falle von Kryptowerte-Transfers nicht reguliert;

    f) Transfers mit selbst gehosteten Adressen;

    g) Transfers von oder an Konten, Adressen oder Wallets, von denen bekannt ist, dass sie mit verdächtigen Aktivitäten in Verbindung stehen;

h) eine negative Bilanz bei der Einhaltung der AML/CFT-Anforderungen des vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette auf der Grundlage öffentlicher Angaben;

i) Transfers von PSP, IPSP, CASP oder ICASP, bei denen festgestellt wurde, dass sie die vorgeschriebenen Angaben wiederholt ohne triftigen Grund nicht zur Verfügung gestellt haben, oder von einem PSP, IPSP, CASP oder ICASP, der zuvor bekanntermaßen mehrfach ohne triftigen Grund die verlangten Angaben nicht übermittelt hat, auch wenn er dies nicht wiederholt versäumt hat;

j) die Verwendung anderer Techniken, um Transaktionen zu schichten, die die Rückverfolgung von Kryptowerten erschweren, indem sie den Weg zum Originator verschleiern, einschließlich, aber nicht nur:

   i) entgegengenommene und rasch weiter transferierte Gelder und Kryptowerte, wodurch die Transferkette künstlich erweitert wird;

   ii) Techniken, Produkte oder Dienstleistungen zur Erhöhung der Anonymität, einschließlich, aber nicht nur Mixer oder Tumbler, Anonymisierer für das Internetprotokoll (IP) und Stealth-Adressen.

48. Bei der Prüfung, ob ein Transfer Anlass zu Verdacht gibt oder nicht, sollten PSP, IPSP, CASP oder ICASP alle mit dem Transfer verbundenen GW-/TF-Risikofaktoren ganzheitlich betrachten und berücksichtigen, dass fehlende oder unzulässige Angaben per se keinen Verdacht auf Geldwäsche oder Terrorismusfinanzierung begründen.

4.5.4. Kontrollen fehlender Angaben gemäß Artikel 7 Absatz 2, Artikel 11 Absatz 2, Artikel 16 Absatz 1 und Artikel 20 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

49. Der PSP des Zahlungsempfängers, der CASP des Begünstigten, der IPSP und der ICASP sollten Angaben als fehlende Angaben behandeln, wenn Felder leer bleiben oder wenn die bereitgestellten Angaben bedeutungslos oder unvollständig sind.

50. Der PSP des Zahlungsempfängers, der CASP des Begünstigten, der IPSP und der ICASP sollten mindestens die folgenden Angaben als bedeutungslos behandeln:

   a) Buchstabenketten aus zufälligen oder unlogischen Buchstaben (z. B. „xxxxx“ oder „ABCDEFG“);

   b) Verwendung von Titeln (wie Dr. oder Frau) ohne den Namen der Person;

   c) andere Bezeichnungen, die inkohärent oder unverständlich sind (z. B. „Ein anderer“ oder „Mein Kunde“).

51. PSP, CASP, IPSP und ICASP, die eine Liste häufig auftretender unsinniger Bezeichnungen führen, die gemeinhin als bedeutungslos angesehen werden, sollten diese regelmäßig überprüfen, um ihre fortdauernde Relevanz zu gewährleisten.

4.6. Transfers mit fehlenden oder unvollständigen Angaben gemäß den Artikeln 8, 12, 17 und 21 der Verordnung (EU) 2023/1113

4.6.1. Risikobasierte Verfahren zur Entscheidung über die Ausführung, Zurückweisung oder Aussetzung eines Transfers gemäß Artikel 8 Absatz 1, Artikel 12, Artikel 17 Absatz 1 und Artikel 21 Absatz 1 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

52. PSP und CASP sollten in ihren Strategien und Verfahren festlegen, wie sie gemäß Artikel 8 Absatz 1, Artikel 12, Artikel 17 Absatz 1 und Artikel 21 der Verordnung (EU) 2023/1113 entscheiden, ob sie einen Transfer zurückweisen, aussetzen oder ausführen. In diesem Zusammenhang sollten PSP und CASP die Risikofaktoren auflisten, die sie bei jedem Transfer berücksichtigen werden.

53. PSP, IPSP, CASP und ICASP sollten bei ihrer Bewertung vor der Entscheidung über das geeignete Vorgehen berücksichtigen, ob gegebenenfalls:

    a) die Angaben die Bestimmung des Gegenstands der Datenübermittlung ermöglichen; und

    b) einer oder mehrere risikoerhöhende Faktoren erkannt wurden, die darauf schließen lassen könnten, dass der Transfer mit einem hohen GW/TF-Risiko verbunden ist oder Anlass zum Verdacht auf GW/TF bietet.

4.6.2. Zurückweisung oder Zurücküberweisung gemäß Artikel 8 Absatz 1 Buchstabe a, Artikel 12 Buchstabe a, Artikel 17 Absatz 1 Buchstabe a und Artikel 21 Absatz 1 Buchstabe a der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

54. Wenn ein IPSP, ein PSP des Zahlungsempfängers, ein ICASP oder ein CASP des Begünstigten beschließt, einen Transfer zurückzuweisen, oder wenn ein ICASP oder ein CASP des Begünstigten beschließt, einen Transfer zurück zu überweisen, anstatt die fehlenden Angaben anzufordern, sollten sie den in der Transferkette vorangehenden PSP, IPSP, CASP oder ICASP darüber informieren, dass der Transfer wegen fehlender Angaben zurückgewiesen oder rücküberwiesen wurde.

Kryptowertetransfers

55. Wenn die Zurückweisung technisch nicht möglich ist, sollte der Transfer an den Originator zurücküberwiesen werden. Ist die Zurücküberweisung an die ursprüngliche Adresse nicht möglich, sollten die CASPs alternative Methoden anwenden. Die alternativen Methoden sollten in ihren Strategien festgelegt werden und das Halten der zurücküberwiesenen Vermögenswerte auf einem sicheren, getrennten Konto sowie die Kommunikation mit dem Originator einschließen und eine geeignete Zurücküberweisungsmethode an den Originator vereinbart werden.

4.6.3. Anforderung der vorgeschriebenen Angaben gemäß Artikel 8 Absatz 1 Buchstabe b, Artikel 12 Absatz 1 Buchstabe b, Artikel 17 Absatz 1 Buchstabe b und Artikel 21 Absatz 1 Buchstabe b der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

56. Wenn der PSP, IPSP, CASP oder ICASP fehlende Angaben anfordert, sollte er eine angemessene Frist für die Bereitstellung der Angaben festlegen. Diese Frist sollte bei Transfers innerhalb der Union drei Arbeitstage und bei Transfers von außerhalb der Union fünf Arbeitstage nicht überschreiten, gerechnet ab dem Tag, an dem der PSP, CASP, IPSP oder ICASP die fehlenden Angaben feststellt. Längere Fristen von bis zu sieben Tagen können festgelegt werden, wenn Transferketten Folgendes umfassen:

    a) mehr als zwei am Transferfluss beteiligte Parteien, darunter Intermediäre und Nichtbanken;

    b) mindestens ein PSP, IPSP, CASP oder ICASP mit Sitz außerhalb der EU.

57. Beschließt ein PSP, IPSP, CASP oder ICASP, die vorgeschriebenen Angaben vom vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette anzufordern, sollte er den vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette über die technischen Maßnahmen unterrichten, die bei diesem Transfer aufgrund fehlender oder unvollständiger Angaben gegebenenfalls ergriffen wurden.

58. Anforderungen von Angaben oder Klarstellungen sollten über dasselbe Nachrichtensystem übermittelt werden, das für die Übermittlung der vorgeschriebenen Angaben verwendet wurde, oder, falls technische Einschränkungen gemäß Absatz 24 bestehen, sichere Kontaktmethoden im Einklang mit den Bestimmungen und Verpflichtungen der Verordnung (EU) 2016/679.

Geldtransfers

59. Wenn die angeforderten Angaben nicht vorliegen, sollte der PSP oder IPSP den vorangehenden PSP oder IPSP in der Transferkette erneut an den vorangehenden PSP oder IPSP verweisen und den vorangehenden PSP oder IPSP in der Transferkette über die Maßnahmen informieren, die

er ergreift, wenn der PSP oder IPSP die angeforderten Angaben nicht innerhalb der festgelegten Frist bereitstellt.

60. Werden die angeforderten Angaben nicht innerhalb der festgelegten Frist zur Verfügung gestellt, sollte der PSP oder IPSP im Einklang mit seinen risikobasierten Strategien und Verfahren gemäß den Absätzen 41 und 42 entscheiden, ob der Transfer zurückgewiesen, ausgesetzt oder ausgeführt wird. Zusätzlich zu dieser Entscheidung sollte er unabhängig davon, ob das Versäumnis wiederholt wurde oder nicht, die künftige Behandlung des vorangehenden PSP oder IPSP in der Transferkette im Hinblick auf die Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung in Erwägung ziehen, einschließlich der Zurückweisung künftiger Transfers von oder an den früheren PSP oder IPSP in der Transferkette oder der Einschränkung oder Beendigung ihrer Geschäftsbeziehung mit diesem PSP oder IPSP.

Kryptowertetransfers

61. Sollten die vorgeschriebenen Angaben nicht vorliegen, sollten CASP oder ICASP im Rahmen der gemäß den Artikeln 17 und 21 der Verordnung (EU) 2023/1113 zu ergreifenden Maßnahmen erwägen, ein Erinnerungsschreiben an den vorangehenden CASP oder ICASP in der Transferkette zu senden und den vorangehenden CASP oder ICASP in der Transferkette über die Maßnahmen zu unterrichten, die sie ergreifen können, falls der CASP oder ICASP die vorgeschriebenen Angaben nicht vor Ablauf der festgelegten Frist bereitstellt.

62. Werden die angeforderten Angaben nicht innerhalb der festgelegten Frist vorgelegt, so sollte der CASP oder ICASP im Einklang mit seinen risikobasierten Strategien und Verfahren gemäß den Absätzen 52 und 53 entscheiden, ob der Transfer zurückgewiesen, zurücküberwiesen, ausgesetzt oder durchgeführt wird. Zusätzlich zu dieser Entscheidung sollte sie unabhängig davon, ob das Versäumnis wiederholt wurde oder nicht, die künftige Behandlung des vorangehenden CASP oder ICASP in der Transferkette im Hinblick auf die Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung erwägen, einschließlich der Zurückweisung künftiger Transfers von oder an den vorangehenden CASP oder ICASP oder die selbst gehostete Adresse in der Transferkette oder der Einschränkung oder Beendigung ihrer Geschäftsbeziehungen mit diesem.

63. Ersuchen um fehlende Angaben oder Klarstellungen in Bezug auf Transfers von selbst gehosteten oder an selbst gehostete Adressen sollten direkt an den Kunden des CASP gerichtet werden.

4.6.4. Ausführung eines Transfers gemäß Artikel 8 Absatz 1, Artikel 12 Absatz 1, Artikel 17 Absatz 1 und Artikel 21 Absatz 1 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

64. Stellt ein PSP, IPSP, CASP oder ICASP fest, dass die vorgeschriebenen Angaben während des Transfers fehlen, unvollständig sind oder unter Verwendung unzulässiger Buchstaben bereitgestellt werden, und führt er den Transfer aus, so sollte er den Grund für die Ausführung des Transfers dokumentieren und im Einklang mit seinen risikobasierten Strategien und Verfahren die künftige Behandlung der vorangehenden PSP, IPSP, CASP, ICASP oder der selbst gehosteten Adresse in der Transferkette für Zwecke der Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung berücksichtigen. Wenn jedoch der Zahler, der Zahlungsempfänger, der Originator oder der Begünstigte aufgrund fehlender oder unvollständiger Angaben oder der mit unzulässigen Buchstaben bereitgestellten Angaben nicht eindeutig identifiziert werden können, sollte der PSP, IPSP, CASP oder ICASP den Transfer nicht ausführen.

4.6.5. Feststellung fehlender oder unvollständiger Angaben nach Ausführung eines Transfers gemäß Artikel 8 Absatz 1, Artikel 12 Absatz 1, Artikel 17 Absatz 1 und Artikel 21 Absatz 1 der Verordnung (EU) 2023/1113

Geldtransfers

65. Stellt ein PSP oder IPSP nachträglich fest, dass die vorgeschriebenen Angaben fehlen, unvollständig oder unter Verwendung unzulässiger Buchstaben bereitgestellt wurden, so sollte er den vorangehenden PSP oder IPSP in der Transferkette auffordern, die fehlenden Angaben unter Verwendung zulässiger Buchstaben oder Einträge gemäß Abschnitt 4.6.3 bereitzustellen.

Kryptowertetransfers

66. Wenn ein CASP oder ICASP den Transfer ausführt und im Nachhinein feststellt, dass die vorgeschriebenen Angaben fehlen oder unvollständig sind, sollte er den vorangehenden CASP oder ICASP in der Transferkette auffordern, die fehlenden Angaben gemäß Abschnitt 4.6.3 zu liefern.

4.7. Wiederholtes Versäumnis von PSP, CASP, IPSP oder ICASP gemäß Artikel 8 Absatz 2, Artikel 12 Absatz 2, Artikel 17 Absatz 2 und Artikel 21 Absatz 2 der Verordnung (EU) 2023/1113

4.7.1. Behandlung von PSP, CASP, IPSP oder ICASP bei wiederholten Versäumnissen gemäß Artikel 8 Absatz 2, Artikel 12 Absatz 2, Artikel 17 Absatz 2 und Artikel 21 Absatz 2 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

67. PSP und CASP sollten in ihren Strategien und Verfahren die quantitativen und qualitativen Kriterien darlegen, anhand derer sie feststellen können, ob ein PSP, IPSP, CASP oder ICASP „wiederholt Versäumnisse aufweist“, und alle Transfers mit fehlenden oder unvollständigen Angaben dokumentieren.

68. Quantitative Kriterien sollten mindestens Folgendes umfassen:

    a) den prozentualen Anteil der von einem bestimmten PSP, IPSP, CASP oder ICASP innerhalb eines bestimmten Zeitraums gesendeten Transfers, bei denen Angaben fehlten; und

    b) den prozentualen Anteil von Nachfragen, die innerhalb der gesetzten Frist nicht oder nicht zufriedenstellend beantwortet wurden.

69. Qualitative Kriterien sollten mindestens Folgendes umfassen:

    a) das Ausmaß der Mitwirkung des PSP, IPSP, CASP oder ICASP in Bezug auf frühere Anforderungen fehlender Angaben;

    b) das Bestehen einer Vereinbarung mit dem PSP, IPSP, CASP oder ICASP, die mehr Zeit für die Bereitstellung der Angaben benötigen;

    c) die Art der fehlenden oder unvollständigen Angaben und die vom PSP, IPSP, CASP oder ICASP angegebenen Gründe dafür, dass die Angaben nicht bereitgestellt wurden.

70. Die Warnung gemäß Artikel 8 Absatz 2 Buchstabe a, Artikel 12 Absatz 2 Buchstabe a, Artikel 17 Absatz 2 Buchstabe a und Artikel 21 Absatz 2 Buchstabe a der Verordnung (EU) 2023/1113 sollte den vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette über die Schritte informieren, die angewandt werden, falls er die vorgeschriebenen Angaben weiterhin nicht bereitstellt, einschließlich der Fristen.

71. PSP und CASP sollten in Erwägung ziehen, dem vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette eine weitere Warnung zukommen zu lassen, dass alle künftigen Transfers zurückgewiesen werden.

72. In Bezug auf die Behandlung gemäß Artikel 8 Absatz 2 Buchstabe b, Artikel 12 Absatz 2 Buchstabe b, Artikel 17 Absatz 2 Buchstabe b und Artikel 21 Absatz 2 Buchstabe b der Verordnung (EU) 2023/1113 sollten PSP und CASP prüfen, wie das wiederholte Versäumnis des vorangehenden PSP, IPSP, CASP oder ICASP in der Transferkette, Angaben bereitzustellen, und wie die Art und Weise des PSP und des CASP, auf solche Anfragen zu reagieren, das mit dem PSP oder CASP verbundene GW/TF-Risiko beeinflusst und gegebenenfalls alle von ihnen erhaltenen Transaktionen in Echtzeit zu überwachen.

73. Vor einer Entscheidung über die Beendigung einer Geschäftsbeziehung, insbesondere, wenn es sich bei dem ihm in der Transferkette vorangehenden PSP, IPSP, CASP oder ICASP um eine Gegenpartei aus einem Drittland handelt, sollte der PSP, IPSP, CASP and ICASP prüfen, ob das Risiko auf andere Weise gemindert werden kann, einschließlich ex ante durch die Anwendung verstärkter Sorgfaltspflichten gemäß Artikel 19 der Richtlinie (EU) 2015/849.

4.7.2. Meldung von PSP, CASP, IPSP oder ICASP bei wiederholten Versäumnissen an die zuständige Behörde gemäß Artikel 8 Absatz 2, Artikel 12 Absatz 2, Artikel 17 Absatz 2 und Artikel 21 Absatz 2 der Verordnung (EU) 2023/1113

Geldtransfers und Kryptowertetransfers

74. Die in Artikel 8 Absatz 2, Artikel 12 Absatz 2, Artikel 17 Absatz 2 und Artikel 21 der Verordnung (EU) 2023/1113 genannte Meldung an die zuständige Behörde sollte von den PSP, IPSP, CASP und ICASP unverzüglich und spätestens drei Monate nach Feststellung von wiederholten Versäumnissen eines PSP, IPSP, CASP oder ICASP übermittelt werden. Die Meldung sollte unabhängig von den Gründen erfolgen, die der PSP, IPSP, CASP oder ICASP bei „wiederholten Versäumnissen“ gegebenenfalls zur Rechtfertigung des Verstoßes angibt, oder von seinem Standort innerhalb oder außerhalb der Union.

75. Der Bericht sollte Folgendes enthalten:

    a) den Namen des PSP, IPSP, CASP oder ICASP, der es wiederholt versäumt hat, die vorgeschriebenen Angaben zu übermitteln;

    b) das Land, in dem der PSP, IPSP, CASP oder ICAS zugelassen ist;

    c) die Art des Verstoßes, einschließlich:

        i. der Häufigkeit von Transfers mit fehlenden Angaben,

        ii. des Zeitraums, innerhalb dessen die Verstöße festgestellt wurden; und

        iii. gegebenenfalls der Gründe, die der PSP, IPSP, CASP oder ICASP für sein wiederholtes Versäumnis, die vorgeschriebenen Angaben zu übermitteln, angeführt hat;

    d) Einzelheiten zu den Schritten, die der meldende PSP, IPSP, CASP oder ICASP unternommen hat.

4.8. Kryptowertetransfers von selbst gehosteten oder an selbst gehostete Adressen gemäß Artikel 14 Absatz 5 und Artikel 16 Absatz 2 der Verordnung (EU) 2023/1113

4.8.1. Individuell identifizierbare Transfers von selbst gehosteten oder an selbst gehostete Adressen gemäß Artikel 14 Absatz 5 und Artikel 16 Absatz 2 der Verordnung (EU) 2023/1113

76. CASP und ICASP sollten den einen Kryptowertetransfer als individuell identifizierbar betrachten, wenn:

    a) eine eindeutige Kennung für jede Überweisung verwendet wird, z. B. einen Transaktions-Hash oder eine Referenznummer; oder

    b) in der Überweisung zusätzliche Angaben enthalten sind, die die Identifizierung des Transfers erleichtern.

4.8.2. Identifizierung eines Transfers von oder an eine selbst gehostete Adresse

77. Um festzustellen, ob am anderen Ende eines Transfers eine selbst gehostete Adresse verwendet wird oder nicht, sollten sich der CASP des Originators und der CASP des Begünstigten auf verfügbare technische Mittel stützen, einschließlich, aber nicht nur Blockchain-Analysen, externe Datenanbieter und Identifikatoren, die von Nachrichtensystemen verwendet werden.

78. Wenn diese Angaben nicht mit technischen Mitteln abgerufen werden können, sollten der CASP des Originators und der CASP des Begünstigten diese Angaben direkt von seinem Kunden erhalten. Stellen in diesem Fall der CASP des Originators und der CASP des Begünstigten fest, dass der Transfer an einen oder von einem anderen CASP erfolgt, sollten der CASP des Originators und der CASP des Begünstigten die notwendigen Schritte unternehmen, um den CASP der Gegenpartei genau zu identifizieren.

79. Der CASP des Originators sollte diese Bewertung vornehmen, bevor der Transfer eingeleitet und die Angaben gemäß Artikel 14 Absatz 5 der Verordnung (EU) 2023/1113 übermittelt werden; der CASP des Begünstigten sollte diese Bewertung vornehmen, bevor die Kryptowerte dem Begünstigten gemäß Artikel 16 Absatz 2 der genannten Verordnung zur Verfügung gestellt werden.

4.8.3. Identifizierung des Originators und des Begünstigten bei einem Transfer von oder an eine selbst gehostete Adresse

80. Wird am anderen Ende des Transfers eine selbst gehostete Adresse verwendet, sollten CASP die Angaben über den Originator oder den Begünstigten von ihrem Kunden einholen.

4.8.4. Transfers über 1 000 EUR und Nachweis des Eigentums oder der Kontrolle über eine selbst gehostete Adresse

81. CASP sollten feststellen, ob sich ein Transfer mit einer selbst gehosteten Adresse auf 1 000 EUR oder mehr beläuft:

    a) zu dem Zeitpunkt, zu dem der Transfer angeordnet oder eingeleitet wurde, im Falle des CASP des Originators; oder

    b) zum Zeitpunkt des Erhalts im Falle des CASP des Begünstigten.

82. Um festzustellen, ob der Wert von Transfers von selbst gehosteten oder an selbst gehostete Adressen 1 000 EUR übersteigt, sollten der CASP den Wechselkurs des zu übertragenden Kryptowertes verwenden, um dessen Wert in Euro zum Zeitpunkt des Transfers zu bestimmen, und zwar unabhängig von etwaigen Transaktionsgebühren.

83. Um zu beurteilen, ob sich die selbst gehostete Adresse im Eigentum oder unter der Kontrolle des Originators oder des Begünstigten befindet, sollten CASP mindestens eine der folgenden Überprüfungsmethoden anwenden:

    a) unbegleitete Überprüfungsverfahren wie in den Leitlinien der EBA über die Nutzung von Anwendungen für den Fern-Kundenannahmeprozess gemäß Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849[9] beschrieben, unter Angabe der Adresse;

    b) begleitete Überprüfungsverfahren wie in den Leitlinien der EBA über die Nutzung von Anwendungen für den Fern-Kundenannahmeprozess gemäß Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849 beschrieben;

    c) Senden eines vordefinierten Betrags (vorzugsweise die kleinste Denominierung eines bestimmten Kryptowerts), der vom CASP festgelegt wird, von der selbst gehosteten und an die selbst gehostete Adresse auf das Konto des CASP;

    d) Aufforderung an den Kunden, eine bestimmte Nachricht im Konto und in der Wallet-Software mit dem Schlüssel, der dieser Adresse entspricht, digital zu signieren;

    e) andere geeignete technische Mittel, solange sie eine zuverlässige und sichere Bewertung ermöglichen und den CASP vollständig davon überzeugen, dass er weiß, wer die Adresse besitzt oder kontrolliert.

84. Die Entscheidung darüber, welche Methode(n) gewählt werden solle(n), sollte von folgenden Faktoren abhängen:

    a) die technischen Fähigkeiten der selbst gehosteten Adresse;

    b) die Robustheit der Bewertung, die jede Methode liefern kann; und

[9] EBA/GL/2022/15.

c) das GW/TF-Risiko.

85. Wenn eine Methode allein nicht zuverlässig genug ist, um die Eigentümerschaft oder Kontrolle einer selbst gehosteten Adresse angemessen zu ermitteln, sollte der CASP eine Kombination von Methoden anwenden.

86. Wenn sich der CASP vollständig davon überzeugt hat, dass sich die selbst gehostete Adresse im Eigentum oder unter der Kontrolle seines Kunden befindet, sollte der CASP dies in seinen Systemen dokumentieren und braucht die oben genannten Maßnahmen möglicherweise nicht erneut auf nachfolgende Transaktionen von/an dieselbe Adresse anwenden („Whitelisting“). Ein CASP, der das „Whitelisting“ verwendet, sollte über Kontrollen verfügen, um Änderungen des GW-/TF-Risikos der selbst gehosteten Adresse und ihrer Eigentümerschaft oder Kontrolle festzustellen. Stellt der CASP fest, dass sich das GW/TF-Risiko der selbst gehosteten Adresse geändert hat oder dass es Hinweise darauf gibt, dass sein Kunde die selbst gehostete Adresse nicht mehr besitzt oder kontrolliert, sollte er diese Adresse aus seiner „Whitelist“ streichen.

4.8.5. Maßnahmen zur Risikominderung bei Transfers von einer selbst gehosteten oder an eine selbst gehostete Adresse

87. Die CASP sollten das Risiko im Zusammenhang mit Transfers von einer selbst gehosteten oder an eine selbst gehostete Adresse gemäß Abschnitt 4.5.3 und im Einklang mit den Leitlinien der EBA zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung bewerten und dabei alle Angaben im Zusammenhang mit Originatoren und Begünstigten, Mustern und geografischen Regionen sowie Informationen von Regulierungsbehörden, Strafverfolgungsbehörden und Dritten nutzen.

88. CASP sollten mindestens eine der in Artikel 19a Absatz 1 der Richtlinie (EU) 2015/849 genannten risikomindernden Maßnahmen anwenden, die den ermittelten Risiken angemessen sind, auch wenn der CASP:

a) Kenntnis davon hat oder erlangt, dass die Angaben über den Originator oder den Begünstigten, der die selbst gehostete Adresse verwendet, falsch sind, oder

b) auf ungewöhnliche oder verdächtige Transaktionsmuster oder Situationen mit erhöhtem GW/TF-Risiko im Zusammenhang mit Übermittlungen mit selbst gehosteten Adressen im Einklang mit den Leitlinien der EBA zu GW/TF-Risikofaktoren stößt.

89. Wird aufgrund der Bewertung in Abschnitt 4.8.4. festgestellt, dass die selbst gehostete Adresse nicht dem Kunden des CASP, sondern einer dritten Person gehört oder von ihr kontrolliert wird, kann die Überprüfung gemäß Artikel 19a Absatz 1 Buchstabe a der Richtlinie (EU) 2015/849 als erfolgt gelten, wenn:

a) der CASP zusätzliche Daten aus anderen Quellen, um die übermittelten Angaben zu überprüfen, sammelt, einschließlich, aber nicht nur Blockchain-Analysedaten, Daten Dritter, Daten anerkannter Behörden und öffentlich verfügbare Informationen, sofern diese zuverlässig und unabhängig sind;

b) der CASP andere geeignete Mittel verwendet, solange der CASP vollständig davon überzeugt ist, dass er die Identität des Originators oder Begünstigten kennt und dies gegenüber seiner zuständigen Behörde nachweisen kann.

90. Wenn solche Transfers den Verdacht auf Geldwäsche und Terrorismusfinanzierung aufwerfen, sollten CASP der zentralen Meldestelle gemäß der Richtlinie (EU) 2015/849 Bericht erstatten.

4.5. Verpflichtungen des PSP des Zahlers, des PSP des Zahlungsempfängers und der IPSP, wenn es sich bei einer Überweisung um einen Lastschrifteinzug handelt

Geldtransfers

91. Handelt es sich bei einem Geldtransfer um eine Lastschrift, sollte der PSP des Zahlungsempfängers dem PSP des Zahlers im Rahmen des Lastschrifteinzugs die vorgeschriebenen Angaben über den Zahler und den Zahlungsempfänger übermitteln. Nach Erhalt dieser Angaben durch den PSP des Zahlers sollten der PSP des Zahlungsempfängers und der IPSP davon ausgehen, dass die Informationspflichten gemäß Artikel 4 Absätze 2 und 4 und Artikel 5 Absätze 1 und 2 der Verordnung (EU) 2023/1113 erfüllt sind.

92. Für die Zwecke des Absatzes 91:

a) sollten die in den Artikeln 4, 5 und 6 der Verordnung (EU) 2023/1113 festgelegten Pflichten auf den PSP des Zahlungsempfängers angewendet werden;

b) die Überprüfung gemäß Artikel 4 Absatz 4 der Verordnung (EU) 2023/1113 sollte vom PSP des Zahlungsempfängers anhand der Angaben zum Zahlungsempfänger vorgenommen werden, bevor er die Lastschrifteinziehung versendet;

c) die in den Artikeln 7, 8 und 9 der Verordnung (EU) 2023/1113 festgelegten Pflichten sollten auf den PSP des Zahlers (Schuldner-PSP) angewandt werden;

d) Die Überprüfung in Artikel 7 Absätze 3 und 4 der Verordnung (EU) 2023/1113 vorgesehene Überprüfung sollte vom PSP des Zahlers (Schuldner-PSP) anhand der Angaben des Zahlers durchgeführt werden, bevor das Konto des Zahlers belastet wird.

93. Stellt der PSP des Zahlers bei Erhalt des Lastschrifteinzugs fest, dass die in den Artikeln 4, 5 und 6 der Verordnung (EU) 2023/1113 genannten Angaben fehlen oder unvollständig sind oder nicht unter Verwendung von Buchstaben oder Einträgen ausgefüllt wurden, die im Einklang mit den Regeln des betreffenden Nachrichtenübermittlungs- oder Zahlungs- und Abwicklungssystem gemäß Artikel 7 Absatz 1 der genannten Verordnung zulässig sind, sollten die in Artikel 8 Absatz 1 Unterabsatz 2 der genannten Verordnung festgelegten Optionen vom PSP des Zahlers angewandt werden. Der PSP des Zahlers sollte sich dafür entscheiden, die vorgeschriebenen Angaben zum Zahler und zum Zahlungsempfänger vor oder nach der Belastung des Kontos des Zahlers nach einem risikobasierten Ansatz anzufordern. Insbesondere sollte er bewerten, ob die Zahlung auch dann gutgeschrieben werden sollte,

wenn Angaben fehlen, oder ob dem Zahlungsempfänger auf der Grundlage von Angaben, die vom Zahler eingeholt und im Rahmen der Due-Diligence-Prüfung des Kunden gemäß Abschnitt 4.4 überprüft wurden, Geld verfügbar gemacht werden sollte.

94. Der PSP des Zahlers sollte die verfügbaren Kommunikationskanäle nutzen, um bei wiederholten Versäumnissen eines PSP des Zahlungsempfängers mit diesem in Kontakt zu treten, bevor er weitere Maßnahmen zur Einschränkung oder Zurückweisung von Zahlungen ergreift. Stützen sich PSP auf Angaben, die sie vor den Transaktionen erhalten haben, sollten ihre Strategien und Verfahren mögliche Änderungen der Angaben im Laufe der Zeit, insbesondere auch Namen und Adressen, berücksichtigen.