

EBA/GL/2024/14

---

14. November 2024

---

## Leitlinien

---

zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten sicherstellen

# 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<sup>1</sup> herausgegeben 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. Leitlinien legen dar, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie nach Ansicht der EBA das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Die gemäß Artikel 4 Nummer 2 der Verordnung (EU) Nr. 1093/2010 zuständigen Behörden sollten die an sie gerichteten Leitlinien einhalten, indem sie sie in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, 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 11.04.2025 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 Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2024/14“ zu übermitteln. Die Mitteilungen 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 auf der Website der EBA veröffentlicht.

---

<sup>1</sup> 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 internen Strategien, Verfahren und Kontrollen festgelegt, die Finanzinstitute, die der Regulierung und Beaufsichtigung gemäß der Richtlinie 2013/36/EU, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG unterliegen, gemäß Artikel 74 Absatz 1 der Richtlinie 2013/36/EU, Artikel 11 Absatz 4 der Richtlinie (EU) 2015/2366 und Artikel 3 Absatz 1 der Richtlinie 2009/110/EG einrichten sollten, um die wirksame Umsetzung der restriktiven Maßnahmen der Union und der Mitgliedstaaten sicherzustellen.

### Adressaten

6. Die vorliegenden Leitlinien richten sich an:
  - (i) zuständige Behörden im Sinne der in Artikel 4 Nummer 2 Ziffer i der Verordnung (EU) Nr. 1093/2010 genannten Rechtsakte;
  - (ii) zuständige Behörden im Sinne von Artikel 4 Nummer 2 Ziffer vi der Verordnung (EU) Nr. 1093/2010 im Hinblick auf die Richtlinie (EU) 2015/2366 und die Richtlinie 2009/110/EG;
  - (iii) Finanzinstitute, die der Regulierung und Beaufsichtigung gemäß der Richtlinie 2013/36/EU, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG unterliegen.
7. Die zuständigen Behörden, die für die Bewertung interner Strategien, Verfahren und Kontrollen zuständig sind, die von Finanzinstituten angenommen wurden, um die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten gemäß dem innerstaatlichen Rechtsrahmen sicherzustellen, können sich bei der Bewertung dieser internen Strategien, Verfahren und Kontrollen auf die vorliegenden Leitlinien stützen.

## Begriffsbestimmung

Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU, der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG verwendeten und definierten Begriffe in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gilt darüber hinaus die folgende Begriffsbestimmung:

### **Restriktive Maßnahmen**

Bezeichnen restriktive Maßnahmen der Union im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2024/1226 und restriktive Maßnahmen der Mitgliedstaaten, die von den Mitgliedstaaten im Einklang mit ihrer nationalen Rechtsordnung erlassen wurden (soweit sie für Finanzinstitute gelten).

---

## 3. Umsetzung

---

### Umsetzungsfrist

8. Diese Leitlinien gelten ab dem 30. Dezember 2025.

## 4. Leitlinien zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten sicherstellen

---

### Allgemeine Bestimmungen

1. Die Finanzinstitute sollten die Bereiche ihrer Geschäftstätigkeit ermitteln und bewerten, die im Hinblick auf restriktive Maßnahmen und die Umgehung restriktiver Maßnahmen besonders anfällig oder exponiert sind. Auf dieser Grundlage sollten sie Strategien, Verfahren und Kontrollen einführen, umsetzen und laufend aktualisieren, um sicherzustellen, dass sie die Regelungen für restriktive Maßnahmen wirksam einhalten können.
2. Diese Strategien, Verfahren und Kontrollen sollten wirksam sein und in einem angemessenen Verhältnis zur Größe, Art und Komplexität des Finanzinstituts und zu seinem Risiko bezüglich restriktiver Maßnahmen stehen.

### 4.1 Rahmen für die Governance und Aufgaben des Leitungsorgans

3. Die Finanzinstitute sollten einen Rahmen für die Governance einrichten, um sicherzustellen, dass die Strategien, Verfahren und Kontrollen für die Umsetzung restriktiver Maßnahmen angemessen sind und wirksam umgesetzt werden.
4. Das Leitungsorgan des Finanzinstituts sollte dafür verantwortlich sein, die Strategie des Finanzinstituts zur Einhaltung restriktiver Maßnahmen zu genehmigen und ihre Umsetzung mittels Strategien, Verfahren und Kontrollen zu überwachen, die erforderlich sind, um die Umsetzung restriktiver Maßnahmen sicherzustellen. Alle Mitglieder des Leitungsorgans sollten sich des Risikos, dem das Finanzinstitut durch restriktive Maßnahmen unterliegt, und seiner Anfälligkeit für die Umgehung restriktiver Maßnahmen bewusst sein.
5. Werden die Geschäfte des Finanzinstituts von einer einzigen Person geführt, so kann diese Person ein Mitglied der oberen Führungsebene mit der Wahrnehmung der Aufgaben des Leitungsorgans nach Absatz 4 beauftragen.

6. Handelt es sich bei dem Finanzinstitut um das Mutterunternehmen einer Gruppe im Sinne von Artikel 2 Nummer 9 und Nummer 11 der Richtlinie 2013/34/EU<sup>2</sup>, sollte das Leitungsorgan des Mutterunternehmens sicherstellen, dass jedes Leitungsorgan, jeder Geschäftsbereich und jede interne Einheit, einschließlich jeder internen Kontrollfunktion der Tochterunternehmen der Gruppe, über die relevanten Informationen verfügt, um restriktive Maßnahmen einhalten zu können. Letztlich sind die einzelnen Unternehmen der Gruppe für die Einhaltung der restriktiven Maßnahmen verantwortlich.
7. Handelt es sich bei einem Finanzinstitut um das Mutterunternehmen einer Gruppe, sollte das Leitungsorgan des Mutterunternehmens sicherstellen, dass die Tochterunternehmen der Gruppe ihre eigenen Risikobewertungen in Bezug auf restriktive Maßnahmen gemäß Abschnitt 4.2 in koordinierter Weise und auf der Grundlage einer gemeinsamen Methodik durchführen, die den Besonderheiten der Gruppe Rechnung trägt.

#### **4.1.1 Aufgaben des Leitungsorgans in seiner Aufsichtsfunktion**

8. Das Leitungsorgan in seiner Aufsichtsfunktion sollte für die Beaufsichtigung und Überwachung des internen Kontroll- und Governance-Rahmens verantwortlich sein, den das Finanzinstitut zur Einhaltung von restriktiven Maßnahmen gemäß Abschnitt 4.3 eingerichtet hat, um sicherzustellen, dass dieser wirksam ist.
9. Zusätzlich zu den Bestimmungen der Leitlinien EBA/GL/2021/05<sup>3</sup> sollte das Leitungsorgan eines Finanzinstituts in seiner Aufsichtsfunktion:
  - a. über die Ergebnisse der letzten Risikobewertung in Bezug auf restriktive Maßnahmen gemäß Abschnitt 4.2 informiert sein;
  - b. im Rahmen der internen Kontrollfunktion beaufsichtigen und überwachen, inwieweit die Strategien und Verfahren für restriktive Maßnahmen gemäß Abschnitt 4.3 angesichts des Risikos durch restriktive Maßnahmen und des Risikos einer Umgehung restriktiver Maßnahmen, dem das Finanzinstitut ausgesetzt ist, angemessen und wirksam sind, und geeignete Schritte unternehmen, um sicherzustellen, dass erforderlichenfalls Korrekturmaßnahmen getroffen werden;
  - c. mindestens einmal jährlich eine Bewertung des wirksamen Funktionierens der Compliance-Funktion für restriktive Maßnahmen durchführen, insbesondere hinsichtlich interner Strategien, Verfahren und Kontrollen, einschließlich der Angemessenheit der für die Einhaltung restriktiver Maßnahmen bereitgestellten personellen und technischen Ressourcen.

---

<sup>2</sup> Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates.

<sup>3</sup> Leitlinien EBA/GL/2021/05 zur internen Governance gemäß der Richtlinie 2013/36/EU.

10. Ist ein Finanzinstitut das Mutterunternehmen einer Gruppe, so sollte das Leitungsorgan dieses Mutterunternehmens auch alle in Absatz 9 genannten Aufgaben auf Gruppenebene wahrnehmen. Letztlich sind die einzelnen Unternehmen der Gruppe für die Einhaltung der restriktiven Maßnahmen verantwortlich.

#### **4.1.2 Aufgaben des Leitungsorgans in seiner Leitungsfunktion**

11. Zusätzlich zu den Bestimmungen der Leitlinien EBA/GL/2021/05 sollte das Leitungsorgan des Finanzinstituts in seiner Leitungsfunktion:
- a. sicherstellen, dass es über die Ergebnisse der letzten Risikobewertung in Bezug auf restriktive Maßnahmen gemäß Abschnitt 4.2 informiert;
  - b. einen angemessenen Rahmen für das Risikomanagement und ein internes Kontrollsystem einrichten, das von der kontrollierten Geschäftstätigkeit hinreichend unabhängig ist;
  - c. Strategien, Verfahren und Kontrollen genehmigen, die in einem angemessenen Verhältnis zu dem Risiko stehen, dem das Finanzinstitut durch die restriktiven Maßnahmen ausgesetzt ist, und die geeignet sind, die Einhaltung der restriktiven Maßnahmen durch das Finanzinstitut zu gewährleisten;
  - d. die wirksame Umsetzung der Verfahren des Finanzinstituts zur Einhaltung der restriktiven Maßnahmen sicherstellen;
  - e. die organisatorische und operative Struktur einrichten, die für die wirksame Umsetzung der vom Leitungsorgan angenommenen Strategie für restriktive Maßnahmen erforderlich ist;
  - f. sicherstellen, dass die personellen und technischen Ressourcen, die für die Einhaltung der restriktiven Maßnahmen bereitgestellt werden, angemessen sind und in einem ausgewogenen Verhältnis zu dem Risiko stehen, dem das Finanzinstitut durch die restriktiven Maßnahmen ausgesetzt ist;
  - g. wenn operative Aufgaben im Zusammenhang mit der Einhaltung restriktiver Maßnahmen ausgelagert werden, sicherstellen, dass diese Vereinbarungen den Leitlinien EBA/GL/2019/02<sup>4</sup> entsprechen, und regelmäßige Berichte des Dienstleisters über die Wirksamkeit des Systems zur Unterrichtung des Leitungsorgans empfangen.
12. Wenn das Finanzinstitut das Mutterunternehmen einer Gruppe ist, sollte das Leitungsorgan dieses Mutterunternehmens sicherstellen, dass alle in Absatz 11 genannten Aufgaben auch auf der Ebene der Tochterunternehmen wahrgenommen werden und dass die festgelegten Strategien und Verfahren mit den Verfahren und Strategien der Gruppe in Einklang stehen, soweit dies nach dem anwendbaren nationalen Recht zulässig ist.

---

<sup>4</sup> Leitlinien EBA/GL/2019/02 zu Auslagerungen, die durch die Leitlinien EBA/GL/XXXX/XX zur zuverlässigen Steuerung des Risikos durch Dritte ersetzt werden sollen.



### **4.1.3 Rolle des leitenden Mitarbeiters, der für die Einhaltung von restriktiven Maßnahmen zuständig ist**

#### 4.1.3.1 Benennung des leitenden Mitarbeiters

13. Die Finanzinstitute sollten einen leitenden Mitarbeiter benennen, der für die Wahrnehmung der in den Absätzen 19 bis 21 aufgeführten Funktionen und Aufgaben zuständig ist. Das Leitungsorgan sollte sicherstellen, dass der leitende Mitarbeiter über die erforderlichen Kenntnisse und das notwendige Verständnis der restriktiven Maßnahmen verfügt, um seine Aufgaben wirksam wahrnehmen zu können.
14. Das Leitungsorgan kann diese Aufgabe einem leitenden Mitarbeiter übertragen, der bereits andere Aufgaben oder Funktionen innerhalb des Finanzinstituts wahrnimmt (z. B. Beauftragter für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung oder leitender Compliance-Beauftragter), sofern:
  - a. dies durch die Größe und Komplexität des Finanzinstituts und das Ergebnis der Risikobewertung in Bezug auf restriktive Maßnahmen gerechtfertigt ist;
  - b. dies nicht die Fähigkeit dieses leitenden Mitarbeiters beeinträchtigt, seine Aufgaben oder Funktionen wirksam wahrzunehmen, und
  - c. diese Kombination von Aufgaben nicht zu Interessenkonflikten führt, wie z. B. Konflikten zwischen operativen Aufgaben und Kontrollaufgaben, die dem betreffenden Mitarbeiter übertragen wurden.
15. Das Leitungsorgan sollte dem leitenden Mitarbeiter gestatten, die in den Absätzen 19 bis 21 genannten Aufgaben anderen Mitarbeitern, die unter der Leitung und Aufsicht des leitenden Mitarbeiters tätig sind, zuzuweisen und zu übertragen, sofern die letztendliche Verantwortung für die wirksame Ausführung dieser Aufgaben bei dem leitenden Mitarbeiter verbleibt.
16. Unabhängig von den institutionellen Regelungen sollten die Finanzinstitute sicherstellen, dass:
  - a. der leitende Mitarbeiter in der Lage ist, die internen Kontrollfunktionen wirksam zu koordinieren und mit ihnen zusammenzuarbeiten; und
  - b. der leitende Mitarbeiter Bericht erstatten kann und direkten Zugang zum Leitungsorgan in seiner Leitungs- und Aufsichtsfunktion hat.
17. Ist das Finanzinstitut Teil einer Gruppe, sollte das Leitungsorgan des Mutterfinanzinstituts einen leitenden Mitarbeiter auf Gruppenebene ernennen.

#### 4.1.3.2 Rolle des leitenden Mitarbeiters

18. Der leitende Mitarbeiter sollte Strategien, Verfahren und Kontrollen entwickeln, einführen und aufrechterhalten, die geeignet sind, die Einhaltung der restriktiven Maßnahmen durch das Finanzinstitut zu gewährleisten, und die in einem angemessenen Verhältnis zu dem Risiko stehen, dem das Finanzinstitut durch restriktive Maßnahmen ausgesetzt ist.

19. Der leitende Mitarbeiter sollte:

- a. die erforderlichen Maßnahmen ergreifen, um die Einhaltung von Abschnitt 4.2 über die Risikobewertung in Bezug auf restriktive Maßnahmen sicherzustellen;
- b. die erforderlichen Maßnahmen ergreifen, um die Einhaltung von Abschnitt 4.3 über wirksame Strategien und Verfahren für restriktive Maßnahmen sicherzustellen;
- c. regelmäßige und angemessene Informationen für das Leitungsorgan bereitstellen, damit dieses seine Aufgaben gemäß Abschnitt 4.1.1 und Abschnitt 4.1.2 wahrnehmen kann; die Informationen für das Leitungsorgan sollten mindestens Folgendes umfassen:
  - i) Änderungen des Risikos, dem das Finanzinstitut durch restriktive Maßnahmen unterliegt, und das Ergebnis der Risikobewertung für das Finanzinstitut in Bezug auf restriktive Maßnahmen;
  - ii) Änderungen der Regelungen für restriktive Maßnahmen und ihre Auswirkungen auf das Finanzinstitut;
  - iii) Statistiken und Informationen in Bezug auf:
    - die Zahl der ausgegebenen Warnmeldungen;
    - die Zahl der zur Analyse anstehenden Warnmeldungen;
    - die Zahl der Meldungen, die der für die Umsetzung der restriktiven Maßnahmen<sup>5</sup> zuständigen nationalen Behörde und/oder der zuständigen Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften übermittelt wurden;
    - die durchschnittliche Zeitspanne zwischen dem echt-positiven Treffer und der Meldung, die der für die Umsetzung der restriktiven Maßnahmen zuständigen nationalen Behörde und/oder der zuständigen Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften übermittelt wurde;
    - den Wert der eingefrorenen Gelder und wirtschaftlichen Ressourcen<sup>6</sup> und die Art dieser bei dem Finanzinstitut gehaltenen Vermögenswerte;
  - iv) Angaben zu den personellen und technischen Ressourcen und deren Angemessenheit im Hinblick auf das Risiko des Finanzinstituts durch restriktive Maßnahmen;
  - v) Mängel oder Unzulänglichkeiten, die im Zusammenhang mit den Strategien, Verfahren und Kontrollen des Finanzinstituts hinsichtlich restriktiver Maßnahmen festgestellt wurden, einschließlich etwaiger Bemerkungen der für die Überwachung der Strategien, Verfahren und Kontrollen in Bezug auf die Umsetzung restriktiver Maßnahmen zuständigen Behörden;
  - vi) Fälle, in denen gegen restriktive Maßnahmen verstoßen oder diese umgangen wurden, und die Gründe für den Verstoß oder die Umgehung;
  - vii) Vorschläge für den Umgang mit Änderungen der aufsichtlichen Anforderungen oder Risiken, die sich aus restriktiven Maßnahmen ergeben, oder mit festgestellten Mängeln oder Unzulänglichkeiten in den Strategien, Verfahren

<sup>5</sup> [https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources\\_en#contact](https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact).

<sup>6</sup> Siehe Artikel 2, Nummer 5 und Nummer 6 der Richtlinie (EU) 2024/1226.

oder Kontrollen des Finanzinstituts in Bezug auf restriktive Maßnahmen sowie mit festgestellten Fällen eines Verstoßes oder einer Umgehung restriktiver Maßnahmen.

- d. Meldung aller Verstöße gegen restriktive Maßnahmen an die für die Umsetzung der restriktiven Maßnahmen zuständigen nationalen Behörden und/oder die zuständige Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften;
  - e. wirksame und konstruktive Zusammenarbeit mit den für die Umsetzung der restriktiven Maßnahmen zuständigen nationalen Behörden und der zuständigen Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften.
20. Wenn das Finanzinstitut Teil einer Gruppe ist, sollte der leitende Mitarbeiter auf Gruppenebene die Wirksamkeit der Strategien, Verfahren und Kontrollen zur Einhaltung der einschlägigen restriktiven Maßnahmen bewerten, und zwar gegebenenfalls über Zweigstellen, Tochterunternehmen, Vermittler, Vertriebsstellen und Agenten hinweg. Letztlich sind die einzelnen Unternehmen der Gruppe für die Einhaltung der restriktiven Maßnahmen verantwortlich.
21. Der leitende Mitarbeiter sollte die Vorbereitung und Durchführung des Schulungsprogramms gemäß Abschnitt 4.4 überwachen.

## 4.2 Durchführung einer Risikobewertung in Bezug auf restriktive Maßnahmen

22. Die internen Verfahren der Finanzinstitute sollten eine Risikobewertung in Bezug auf restriktive Maßnahmen umfassen, um zu verstehen, inwieweit die einzelnen Geschäftsbereiche von restriktiven Maßnahmen betroffen und anfällig für die Umgehung restriktiver Maßnahmen sind.
23. Die Risikobewertung in Bezug auf restriktive Maßnahmen sollte es den Finanzinstituten ermöglichen, Folgendes zu ermitteln und zu bewerten:
- a. welche Regelungen für restriktive Maßnahmen für sie gelten;
  - b. die Wahrscheinlichkeit, dass restriktive Maßnahmen nicht umgesetzt werden;
  - c. die Wahrscheinlichkeit, dass restriktive Maßnahmen umgangen werden;
  - d. die Auswirkungen etwaiger Verstöße gegen restriktive Maßnahmen und
  - e. die folgenden Risikofaktoren:
    - a) geografisches Risiko, einschließlich:
      - i. der Standorte der Geschäftstätigkeit des Finanzinstituts, d. h. die Rechtsordnungen und Gebiete, in denen das Finanzinstitut niedergelassen oder tätig ist;
      - ii. des Ausmaßes, in dem diese Rechtsordnungen und Gebiete restriktiven Maßnahmen unterliegen oder bekanntermaßen dazu genutzt werden, restriktive Maßnahmen zu umgehen;

iii. des Ursprungs- und Bestimmungsorts der Transaktionen.

b) Kundenrisiko, einschließlich:

- i. Verbindungen der Kunden und gegebenenfalls ihrer wirtschaftlichen Eigentümer und der herrschenden Anteilseigner zu Ländern, gegen die aufgrund der Lage in diesen Ländern restriktive Maßnahmen verhängt wurden oder von denen bekannt ist, dass sie zur Umgehung restriktiver Maßnahmen genutzt werden;
- ii. der Zahl der Kunden, die Art der Kunden und die Komplexität dieser Kunden, wie z. B. Schwierigkeiten bei der Feststellung der Identität des wirtschaftlichen Eigentümers;
- iii. der Geschäftstätigkeit des Kundenstamms und die Komplexität der Geschäftstätigkeit, einschließlich etwaiger Verbindungen zu Wirtschaftszweigen oder Sektoren, die Gegenstand wirtschaftlicher oder sonstiger restriktiver Maßnahmen sein können, sowie die Häufigkeit und die Art der Transaktionen.

c) Produkt- und Dienstleistungsrisiko, einschließlich:

- i. der Art der Produkte und Dienstleistungen des Finanzinstituts;
- ii. des Ausmaßes, in dem das Finanzinstitut durch die Bereitstellung dieser Produkte und Dienstleistungen dem Risiko von Verstößen gegen restriktive Maßnahmen und der Umgehung dieser Maßnahmen ausgesetzt ist;

d) Vertriebskanalrisiko, einschließlich der Frage, ob der Einsatz von Vermittlern, Agenten, Dritten, Korrespondenzbankbeziehungen oder anderen Vertriebskanälen zu Schwachstellen führt, unter anderem durch:

- i. Beschränkung der Sichtbarkeit von beteiligten Parteien für das Finanzinstitut;
- ii. Abhängigkeit des Finanzinstituts von durch Dritten durchgeführten Überprüfungsverfahren;
- iii. Erhöhung der Anfälligkeit des Finanzinstituts für geografische Risiken, weil es in Ländern tätig ist oder seinen Sitz hat, gegen die aufgrund der Lage in diesen Ländern restriktive Maßnahmen verhängt wurden oder von denen bekannt ist, dass sie zur Umgehung restriktiver Maßnahmen genutzt werden.

24. Die in Absatz 22 genannte Bewertung sollte sich auf ein ausreichend breites Spektrum von Informationsquellen stützen, darunter mindestens die Folgenden:

- a. Informationen, die das Finanzinstitut im Rahmen der Anwendung der Sorgfaltspflichten gegenüber Kunden in Übereinstimmung mit den Regelungen des Artikels 13 der Richtlinie (EU) 2015/849 erlangt hat;
- b. Informationen von internationalen Stellen, staatlichen Stellen, zuständigen nationalen Behörden, einschließlich der für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständigen Finanzaufsichtsbehörden, zentralen

- Meldestellen für Finanztransaktionsuntersuchungen und Strafverfolgungsbehörden, wie z. B. aktuelle Typologien zur Umgehung restriktiver Maßnahmen;
- c. Informationen aus glaubwürdigen und zuverlässigen öffentlichen Quellen, z. B. Berichte in angesehenen Zeitungen und sonstigen renommierten Medien;
  - d. Informationen von glaubwürdigen und zuverlässigen gewerblichen Einrichtungen, z. B. Risikoberichte;
  - e. falls verfügbar, eine Analyse früherer Warnmeldungen bezüglich restriktiver Maßnahmen mit Blick auf echt-positive und falsch-positive Treffer, um Situationen zu ermitteln, in denen echt-positive Treffer am wahrscheinlichsten sind.
25. Bei der Risikobewertung in Bezug auf restriktive Maßnahmen sollten die Finanzinstitute prüfen, ob eine rückwirkende Überprüfung ihrer Kundendatenbank und der Aufzeichnungen über frühere Transaktionen sinnvoll und verhältnismäßig sein könnte. Dies kann der Fall sein, wenn das Finanzinstitut festgestellt hat oder berechtigten Grund zu der Annahme hat, dass sein bisheriges Überprüfungsverfahren unzureichend oder unwirksam war.
26. Die Finanzinstitute sollten sicherstellen, dass ihre Risikobewertung in Bezug auf restriktive Maßnahmen aktuell und relevant bleibt. Um dieses Ziel zu erreichen, sollten die Finanzinstitute sie mindestens einmal jährlich überprüfen und gegebenenfalls aktualisieren. Darüber hinaus sollten die Finanzinstitute ihre Risikobewertung in Bezug auf restriktive Maßnahmen gegebenenfalls in folgenden Fällen überprüfen:
- a. Annahme neuer restriktiver Maßnahmen und wesentliche Änderungen bestehender restriktiver Maßnahmen;
  - b. vor der Einführung neuer Produkte, dem Angebot neuer Produktvertriebskanäle, der Bedienung neuer Kundengruppen und dem Eintritt in neue geografische Gebiete;
  - c. wesentliche Änderungen des Tätigkeitsprofils, des Kundenstamms, der Organisationsstruktur oder des Geschäftsmodells des Instituts;
  - d. die Feststellung, dass restriktive Maßnahmen nicht umgesetzt oder umgangen wurden, was die Unangemessenheit der Risikobewertung in Bezug auf restriktive Maßnahmen deutlich macht;
  - e. Mängel bei der Risikobewertung bestehender restriktiver Maßnahmen, die von dem Finanzinstitut oder der zuständigen Behörde festgestellt wurden, die für die Beaufsichtigung der internen Strategien, Verfahren und Kontrollen zur Sicherstellung der Umsetzung der restriktiven Maßnahmen der Union und der Mitgliedstaaten verantwortlich ist.
27. Die Finanzinstitute sollten ihre Methodik zur Durchführung und Überprüfung ihrer Risikobewertung in Bezug auf restriktive Maßnahmen sowie die Ergebnisse dieser Bewertung dokumentieren und sie ihrer zuständigen Behörde auf Anfrage zur Verfügung stellen.

28. Handelt es sich bei dem Finanzinstitut um das Mutterunternehmen einer Gruppe, so sollte das Leitungsorgan der Gruppe sicherstellen, dass die Tochterunternehmen der Gruppe ihre eigene Risikobewertung in Bezug auf restriktive Maßnahmen koordiniert und auf der Grundlage einer gemeinsamen Methodik unter Berücksichtigung ihrer jeweiligen Besonderheiten durchführt.

### 4.3 Sicherstellung der laufenden Wirksamkeit der Strategien, Verfahren und Kontrollen für restriktive Maßnahmen

29. Um wirksam zu sein, sollten die Strategien, Verfahren und Kontrollen eines Finanzinstituts zur Umsetzung restriktiver Maßnahmen das Finanzinstitut in die Lage versetzen, alle geltenden restriktiven Maßnahmen unverzüglich, vollständig und ordnungsgemäß umzusetzen.

30. Die Strategien, Verfahren und Kontrollen sollten mindestens Folgendes abdecken:

- a. Prozesse, mit denen sichergestellt wird, dass die Finanzinstitute über aktuelle Informationen über geltende restriktive Maßnahmen verfügen;
- b. Prozesse, mit denen sichergestellt wird, dass die Listen und Anforderungen der geltenden restriktiven Maßnahmen aktualisiert werden, sobald diese in Kraft treten;
- c. Prozesse, mit denen sichergestellt wird, dass die Risikobewertung in Bezug auf restriktive Maßnahmen relevant und aktuell bleibt;
- d. Prozesse, mit denen sichergestellt wird, dass die Strategien, Verfahren und Kontrollen mit der Risikobewertung in Bezug auf restriktive Maßnahmen in Einklang stehen;
- e. Prozesse, mit denen sichergestellt wird, dass Strategien und Verfahren für restriktive Maßnahmen:
  - i. regelmäßig überprüft werden;
  - ii. bei Bedarf regelmäßig überprüft und aktualisiert werden;
  - iii. wirksam umgesetzt und
  - iv. so gestaltet sind, dass bei der Feststellung von Mängeln die erforderlichen Maßnahmen ausgelöst werden.
- f. Verfahren zur Einleitung einer unverzüglichen Untersuchung aller potenziellen Treffer;
- g. im Falle eines echt-positiven Treffers Verfahren, die Folgemaßnahmen auslösen, um die Einhaltung der geltenden restriktiven Maßnahmen zu gewährleisten, einschließlich der unverzüglichen Ablehnung, Aussetzung oder des Einfrierens von Geldern, sowie Meldung an die für die Umsetzung der restriktiven Maßnahme zuständigen nationalen Behörden oder an die zuständige Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften innerhalb der von diesen Behörden oder in der geltenden Verordnung über restriktive Maßnahmen festgesetzten Fristen;
- h. eine dokumentierte interne Organisation, in der die Aufgaben und Verantwortlichkeiten im Zusammenhang mit restriktiven Maßnahmen klar festgelegt sind, auch im Falle einer Auslagerung;
- i. sonstige Aspekte gemäß den Leitlinien EBA/GL/2024/15 zu internen Strategien, Verfahren und Kontrollen zur Sicherstellung der Umsetzung restriktiver Maßnahmen gemäß der Verordnung (EU) 2023/1113.

## 4.4 Schulungen

31. Die Finanzinstitute sollten ihren Mitarbeitern regelmäßig Schulungen anbieten, um sicherzustellen, dass sie mit den folgenden Aspekten vertraut sind und es auch bleiben:
  - a. geltende restriktive Maßnahmen;
  - b. das Ergebnis der Risikobewertung in Bezug auf restriktive Maßnahmen und
  - c. Strategien, Verfahren und Kontrollen zur Einhaltung von geltenden restriktiven Maßnahmen.
  
32. Die Schulungen sollten auf die Mitarbeiter und ihre konkrete Aufgabe zugeschnitten sein. Sie sollten aktuell und angemessen sein, damit das Finanzinstitut in der Lage ist, die restriktiven Maßnahmen einzuhalten. Innerhalb einer Gruppe kann diese Tätigkeit ganz oder teilweise von der Muttergesellschaft ausgeführt werden.
  
33. Die Finanzinstitute sollten ihren Schulungsplan dokumentieren und auf Anfrage der zuständigen Behörde nachweisen können, dass ihre Schulung angemessen und wirksam ist.

EBA/GL/2024/15

---

14. November 2024

---

## Leitlinien

---

zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten gemäß der Verordnung (EU) 2023/1113 sicherstellen



# 1. Verpflichtung zur Einhaltung der Leitlinien und Meldepflichten

---

## Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 <sup>7</sup> herausgegeben wurden. Gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden, Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen alle erforderlichen Anstrengungen unternehmen, um den Leitlinien nachzukommen.
2. Leitlinien legen dar, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie nach Ansicht der EBA das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Zuständige Behörden im Sinne von Artikel 4 Nummer 2 der Verordnung (EU) Nr. 1093/2010 sollten die für sie geltenden Leitlinien einhalten, indem sie sie 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 11.04.2025 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 Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2024/15“ zu übermitteln. Die Mitteilungen 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 auf der Website der EBA veröffentlicht.

---

<sup>7</sup> 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 internen Strategien, Verfahren und Kontrollen festgelegt, die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen einrichten sollten, um die wirksame Umsetzung der restriktiven Maßnahmen der Union und der Mitgliedstaaten bei der Durchführung von Geldtransfers und Kryptowertetransfers im Sinne der Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates<sup>8</sup> sicherzustellen.

### Adressaten

6. Die vorliegenden Leitlinien richten sich an:
  - a. die zuständigen Behörden, die die Einhaltung der sich aus der Verordnung (EU) 2023/1113 ergebenden Pflichten durch Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen überwachen;
  - b. Finanzinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 1093/2010, die Zahlungsdienstleister im Sinne von Artikel 3 Nummer 5 der Verordnung (EU) 2023/1113 und Anbieter von Krypto-Dienstleistungen im Sinne von Artikel 3 Nummer 15 der Verordnung (EU) 2023/1113 sind.

---

<sup>8</sup> 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 (Neufassung) (ABl. L 150 vom 9.6.2023, S. 1).

## Begriffsbestimmungen

7. Die in der Verordnung (EU) 2023/1113 verwendeten und definierten Begriffe haben in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

<b>Restriktive Maßnahmen</b>	Bezeichnen restriktive Maßnahmen der Union im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2024/1226 und restriktive Maßnahmen der Mitgliedstaaten, die von den Mitgliedstaaten im Einklang mit ihrer nationalen Rechtsordnung erlassen wurden (soweit sie für Finanzinstitute gelten).
<b>Gezielte finanzielle Sanktionen</b>	Bezeichnen sowohl das Einfrieren von Vermögenswerten als auch das Verbot, Gelder oder andere Vermögenswerte unmittelbar oder mittelbar zugunsten der Personen und Organisationen bereitzustellen, die in Beschlüssen des Rates auf der Grundlage von Artikel 29 EUV und in Verordnungen des Rates auf der Grundlage von Artikel 215 AEUV benannt wurden.
<b>Sektorspezifische restriktive Maßnahmen</b>	Bezeichnen restriktive Maßnahmen wie Embargos für Waffen und Rüstungsgüter oder wirtschaftliche und finanzielle Maßnahmen (z. B. Ein- und Ausfuhrbeschränkungen oder Beschränkungen für die Erbringung bestimmter Dienstleistungen wie Bankdienstleistungen).

## 3. Umsetzung

---

### Umsetzungsfrist

8. Diese Leitlinien gelten ab dem 30. Dezember 2025.

## 4. Leitlinien zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten gemäß der Verordnung (EU) 2023/1113 sicherstellen

---

### Allgemeine Bestimmungen

1. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten Strategien, Verfahren und Kontrollen zur Einhaltung restriktiver Maßnahmen einrichten. Diese Strategien, Verfahren und Kontrollen sollten sich an den Leitlinien EBA/GL/2024/14 zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten sicherstellen, orientieren.
2. Diese Strategien, Verfahren und Kontrollen sollten es den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen ermöglichen, Betroffene zu identifizieren, die restriktiven Maßnahmen unterliegen. Sie sollten es den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen auch ermöglichen, die erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass sie diesen Betroffenen keine Gelder oder Kryptowerte zur Verfügung stellen, keine Finanztransaktionen für sie durchführen und keine Dienstleistungen für sie erbringen, die durch restriktive Maßnahmen verboten sind, und dass sie das Risiko einer Umgehung restriktiver Maßnahmen steuern.

### 4.1 Überprüfung restriktiver Maßnahmen

3. Die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten ein wirksames Überprüfungssystem einrichten, um die Ziele restriktiver Maßnahmen zuverlässig zu ermitteln, wie in Abschnitt 4.4 näher ausgeführt wird.

#### **4.1.1 Wahl des Überprüfungssystems**

4. Die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten auf der Grundlage ihrer Risikobewertung in Bezug auf restriktive Maßnahmen entscheiden, welches Überprüfungssystem sie verwenden, oder das von ihnen verwendete Überprüfungssystem validieren, um die geltenden restriktiven Maßnahmen einzuhalten. Das Überprüfungssystem sollte an die Größe, Art und Komplexität der Geschäftstätigkeit der Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen und an das jeweilige Risiko, dem diese aufgrund der restriktiven Maßnahmen ausgesetzt sind, angepasst sein.
5. Bei der Entscheidung über ihr Überprüfungssystem sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen berücksichtigen, ob sie Zugang zu den Ressourcen haben, die für den wirksamen Einsatz des gewählten Systems erforderlich sind.
6. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten die Leistungsfähigkeit des Überprüfungssystems regelmäßig kontrollieren, um sicherzustellen, dass es weiterhin wirksam ist und die Ziele restriktiver Maßnahmen weiterhin zuverlässig identifiziert. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten das verwendete Überprüfungssystem mindestens einmal jährlich und unverzüglich überprüfen, wenn sie Grund zu der Annahme haben, dass das System für den beabsichtigten Zweck ungeeignet sein könnte.
7. Gemäß Artikel 8 der Verordnung (EU) 2022/2554 sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen die Fähigkeiten und Anwendungsgrenzen des Überprüfungssystems kennen und dokumentieren. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in der Lage sein, gegenüber ihren zuständigen Behörden nachzuweisen, dass ihr Überprüfungssystem angemessen ist.

#### **4.1.2 Verwaltung von Listen**

8. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, welche restriktiven Maßnahmen sie anzuwenden haben.
9. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten über Strategien und Verfahren verfügen, um
  - a. festzustellen, wann ein neues Paket restriktiver Maßnahmen angenommen oder eine bestehende restriktive Maßnahme aktualisiert oder aufgehoben wird;
  - b. ihre gemäß Abschnitt 4.1.3 zu überprüfenden internen Daten ohne unangemessene Verzögerung nach dem Inkrafttreten einer neuen restriktiven Maßnahme oder nach der Aktualisierung oder Aufhebung einer bestehenden restriktiven Maßnahme aktualisieren.

### 4.1.3 Festlegung der zu prüfenden Daten

10. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, welche Arten von Daten sie für jede Art von restriktiven Maßnahmen überprüfen, wobei sie das Ergebnis ihrer Risikobewertung in Bezug auf restriktive Maßnahmen und die restriktiven Maßnahmen, die sie anwenden müssen, berücksichtigen.
11. Bei der Entscheidung, welche Daten im Hinblick auf die Art der anzuwendenden restriktiven Maßnahme zu überprüfen sind, sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen alle in ihrem Besitz befindlichen Daten über ihre Kunden berücksichtigen, einschließlich der Informationen, die sie erhalten haben:
  - a. bei der Anwendung der Sorgfaltspflichten gegenüber Kunden gemäß dem Unionsrecht und dem nationalen Recht zur Umsetzung des Unionsrechts und
  - b. bei der Einhaltung der Verordnung (EU) 2023/1113.
12. Im Einklang mit den Anforderungen der Verordnung (EU) 2023/1113 sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen bewerten, ob die in ihrem Besitz befindlichen Daten hinreichend genau, aktuell und detailliert sind, um feststellen zu können, ob eine an dem Transfer beteiligte Partei, ihr wirtschaftlicher Eigentümer oder eine Person, die vorgibt, in ihrem Namen zu handeln, oder dazu befugt ist, restriktiven Maßnahmen unterliegt.
13. Um wiederholte falsche Warnmeldungen in Bezug auf eine natürliche oder juristische Person, Organisation oder Einrichtung zu vermeiden, die keinen restriktiven Maßnahmen unterliegt, aber durch das bestehende Überprüfungssystem fälschlicherweise als solche identifiziert wurde, können Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen beschließen, diese Personen in eine spezielle interne Liste aufzunehmen (Whitelisting). Die Gründe für eine solche Entscheidung sind zu dokumentieren. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten eine solche Liste ohne unangemessene Verzögerung nach dem Inkrafttreten einer neuen oder geänderten restriktiven Maßnahme oder bei Änderung der Kundendaten überprüfen.

### 4.1.4 Überprüfung des Kundenstamms

14. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, wie sie ihren Kundenstamm überprüfen.
15. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten ihre gesamte Kundendatenbank regelmäßig überprüfen und die Häufigkeit dieser Kundenüberprüfung auf der Grundlage ihrer Risikobewertung in Bezug auf restriktive Maßnahmen festlegen.
16. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in einer internen Entscheidung festlegen, bei welchen auslösenden Ereignissen stets eine Überprüfung ihrer

Kunden erfolgen sollte, und diese Entscheidungen auf dem neuesten Stand halten. Als auslösende Ereignisse werden mindestens die folgenden Ereignisse angesehen:

- a. eine Änderung einer der bestehenden Benennungen oder restriktiven Maßnahmen, eine neue Benennung oder das Inkrafttreten einer neuen restriktiven Maßnahme;
- b. bei Aufnahme einer Kundenbeziehung oder vor Beginn einer Geschäftsbeziehung;
- c. bei wesentlichen Änderungen der Daten in Bezug auf die Sorgfaltspflichten gegenüber einem bestehenden Kunden, wie z. B. Änderung des Namens, des Sitzes, der Staatsangehörigkeit oder Änderung der Geschäftstätigkeit;
- d. wenn hinreichender Grund zu der Annahme besteht, dass der Kunde oder eine Person, die vorgibt oder befugt ist, im Namen des Kunden zu handeln, versucht, restriktive Maßnahmen zu umgehen.

17. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten im Einklang mit den geltenden restriktiven Maßnahmen mindestens die folgenden Kundeninformationen überprüfen:

- a. im Falle einer natürlichen Person:
  - a. den Vor- und Nachnamen im Original und/oder in Transliteration und
  - b. das Geburtsdatum.
- b. im Falle einer juristischen Person: den Namen der juristischen Person im Original und/oder in Transliteration;
- c. im Falle einer natürlichen oder juristischen Person, Einrichtung oder Organisation: alle sonstigen Namen, Aliasnamen, Handelsnamen oder Adressen einer elektronischen Geldbörse, sofern diese in den entsprechenden Listen im Zusammenhang mit restriktiven Maßnahmen aufgeführt sind. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten mittels der Risikobewertung in Bezug auf restriktive Maßnahmen ordnungsgemäß begründen, warum sie sich dafür entschieden haben, diese Informationen nicht zu überprüfen, sofern diese verfügbar sind.

18. Bei der Überprüfung von Kunden, bei denen es sich um juristische Personen, natürliche Personen, Einrichtungen oder Organisationen handelt, sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen, soweit die Informationen verfügbar sind, auch Folgendes überprüfen:

- a. wirtschaftliche Eigentümer durch Eigentumsbeteiligung;
- b. wirtschaftliche Eigentümer durch Kontrolle;
- c. jede Person, die vorgibt oder befugt ist, im Namen des Kunden zu handeln.

#### **4.1.5 Überprüfung von Geldtransfers und Kryptowertetransfers**

19. Mit Ausnahme der in Artikel 5d der Verordnung (EU) Nr. 260/2012 genannten Fälle sollten Zahlungsdienstleister Geldtransfers überprüfen, bevor sie dem Begünstigten die Gelder zur Verfügung stellen, und Anbieter von Krypto-Dienstleistungen sollten alle Transfers von Kryptowerten überprüfen, bevor sie dem Begünstigten die Kryptowerte zur Verfügung stellen,



und zwar unabhängig davon, ob sie im Rahmen einer Geschäftsbeziehung oder als Teil einer einmaligen Transaktion erfolgen.

20. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten alle Parteien, die an Geldtransfers oder Kryptowertetransfers beteiligt sind, im Hinblick auf geltende restriktive Maßnahmen überprüfen. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten bei ihrer Risikobewertung in Bezug auf restriktive Maßnahmen besonderes Augenmerk auf die Stichhaltigkeit und Zuverlässigkeit der Strategien und Verfahren für restriktive Maßnahmen legen, die von den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen, mit denen sie Geschäfte tätigen, eingeführt wurden, um die Einhaltung der restriktiven Maßnahmen zu sicherzustellen.
21. Alle Daten, die für die Beurteilung der Frage, ob eine Transaktion von geltenden restriktiven Maßnahmen betroffen sein könnte, relevant sein können, sollten mit geltenden restriktiven Maßnahmen abgeglichen werden. Die zu überprüfenden Daten sollten mindestens Folgendes umfassen:
  - a. Angaben zum Zahler und zum Zahlungsempfänger gemäß Artikel 4 der Verordnung (EU) 2023/1113;
  - b. Angaben zum Originator und zum Begünstigten gemäß Artikel 14 der Verordnung (EU) 2023/1113;
  - c. Zweck des Geldtransfers oder Transfers von Kryptowerten und, soweit verfügbar und vorbehaltlich einer Risikobewertung in Bezug auf restriktive Maßnahmen, weitere Freitextfelder mit zusätzlichen Angaben zum tatsächlichen Absender/Empfänger der Geldbeträge oder der Kryptowerte;
  - d. Angaben zu den am Geldtransfer oder Kryptowertetransfer beteiligten Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen, einschließlich zwischengeschalteter Institute und Korrespondenzbanken, mit Überprüfung von Identifikationscodes wie BIC, SWIFT oder anderen;
  - e. sonstige Angaben zum Geldtransfer oder Kryptowertetransfer, je nach Art und Typ des Vorgangs und der erhaltenen Belege, sofern Informationen verfügbar sind, und vorbehaltlich einer Risikobewertung in Bezug auf restriktive Maßnahmen;
  - f. Adressen der elektronischen Geldbörsen des Originators und des Begünstigten eines Transfers von Kryptowerten, soweit diese Informationen in den offiziellen Listen der Adressen von elektronischen Geldbörsen, die restriktiven Maßnahmen unterliegen, verfügbar sind.
22. Im Einklang mit den Bestimmungen in Abschnitt 4.6 der Leitlinien EBA/GL/2024/11 zu Informationspflichten in Bezug auf Geldtransfers und Transfers bestimmter Kryptowerte gemäß der Verordnung (EU) 2023/1113 („Leitlinien zur Transferregelung“) sollten alle neuen Informationen, die nachträglich, vor oder nach der Ausführung des Transfers, erlangt werden, ebenfalls geprüft werden.

23. Wenn es aufgrund des Volumens und der Anzahl der Transfers von Kryptowerten angemessen ist, sollten die Anbieter von Krypto-Dienstleistungen in Erwägung ziehen, eine Blockchain-Analyse zum Zwecke der Transaktionsüberwachung in den bestehenden Rahmen zu integrieren.

#### **4.1.6 Kalibrierung**

24. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten festlegen, wie die Einstellungen eines automatisierten Überprüfungssystems kalibriert werden können, um die Qualität der Warnmeldungen zu maximieren und eine eindeutige Identifizierung zu ermöglichen und gleichzeitig die Einhaltung restriktiver Maßnahmen sicherzustellen. Auf der Grundlage ihrer Risikobewertung in Bezug auf restriktive Maßnahmen und der regelmäßigen Durchführung von Tests sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen mindestens folgende Maßnahmen ergreifen:

- a. für jede anwendbare restriktive Maßnahme Festlegung geeigneter Parameter bezogen auf die Treffer, die geeignet sind, eine angemessene Warnmeldung zu erzeugen, die es den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen ermöglicht, ihren Verpflichtungen in Bezug auf restriktive Maßnahmen nachzukommen, indem die Schwellenwerte für echt-positive Ergebnisse in Verbindung mit verschiedenen Prozentsätzen der Treffer überprüft werden. Die Kalibrierung sollte weder zu empfindlich sein, da dies zu einer hohen Zahl von falsch-positiven Treffern führen würde, noch zu ungenau sein, da dies zur Folge hätte, dass benannte Personen, Organisationen und Einrichtungen nicht identifiziert oder frei verfügbare Informationen nicht für andere restriktive Maßnahmen genutzt werden;
- b. Verwendung eines Überprüfungssystems, das eine algorithmenbasierte Technik ermöglicht, die einen Namen oder eine Wortfolge abgleichen kann, wenn der Inhalt der zu überprüfenden Information nicht identisch ist, aber die Schreibweise, das Muster oder der Klang eine enge Übereinstimmung mit dem Inhalt eines für die Überprüfung verwendeten Datensatzes aufweist („Fuzzy Matching“), und Kalibrierung des Grades des „Fuzzy Matching“ in ihrem Überprüfungssystem.

25. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten sowohl vor der Entwicklung eines neuen Überprüfungssystems als auch regelmäßig im Einklang mit ihrer Risikobewertung in Bezug auf restriktive Maßnahmen eine entsprechende Entscheidung über die Kalibrierung treffen. Sie sollten ihre Begründung dokumentieren und sie den zuständigen Behörden auf Anfrage zur Verfügung stellen.

#### **4.1.7 Inanspruchnahme Dritter und Auslagerung**

26. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren die Maßnahmen festlegen, die von den Zahlungsdienstleistern, Anbietern von Krypto-Dienstleistungen oder ausgelagerten Dienstleistern zu ergreifen sind, um die Einhaltung der geltenden restriktiven Maßnahmen zu gewährleisten. Für die Auslagerung von Dienstleistungen sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen,

gegebenenfalls unter Berücksichtigung der Leitlinien EBA/GL/2019/02<sup>9</sup>, die folgenden wesentlichen Grundsätze anwenden:

- a. Letztendlich liegt die Verantwortung für die Einhaltung von restriktiven Maßnahmen, ungeachtet dessen, ob bestimmte Funktionen ausgelagert sind oder nicht, beim Zahlungsdienstleister oder Anbieter von Krypto-Dienstleistungen.
  - b. Die Rechte und Pflichten des Zahlungsdienstleisters oder Anbieters von Krypto-Dienstleistungen sollten eindeutig festgelegt und schriftlich festgehalten sein.
  - c. Der Zahlungsdienstleister oder Anbieter von Krypto-Dienstleistungen, der sich auf eine Auslagerungsvereinbarung stützt, sollte weiterhin für die Überwachung und Aufsicht der Qualität der vom Dienstleister erbrachten Dienstleistungen verantwortlich bleiben.
  - d. Für gruppeninterne Auslagerungen sollte derselbe regulatorische Rahmen gelten wie für Auslagerungen an Dienstleistungserbringer außerhalb der Gruppe.
27. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten die erforderlichen Kontrollen einführen und anwenden, um sicherzustellen, dass sie durch die Inanspruchnahme ausgelagerter Dienstleister nicht dem Risiko eines Verstoßes gegen restriktive Maßnahmen ausgesetzt sind, und diese Kontrollen in der Auslagerungsvereinbarung dokumentieren.
28. Wenn die Dienstleister die von Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen zu verwendenden Daten in Bezug auf natürliche Personen, juristische Personen, Organisationen und Einrichtungen, die geltenden restriktiven Maßnahmen unterliegen, aktualisieren, sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sicherstellen, dass durch eine Dienstleistungsvereinbarung das Risiko von Verstößen gegen restriktive Maßnahmen durch die Zahlungsdienstleister oder Anbieter von Krypto-Dienstleistungen minimiert wird.
29. Wenn Auslagerungsvereinbarungen bestehen, sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen regelmäßig überprüfen, ob der Dienstleister seinen Verpflichtungen aus der Vereinbarung nachkommt, sie sollten die Wirksamkeit der unter die Vereinbarung fallenden Dienstleistungen bewerten und alle erforderlichen Korrekturmaßnahmen ergreifen, einschließlich der Neuverhandlung der Vereinbarung.
30. Die Bestimmungen dieses Abschnitts berühren nicht die Pflichten und Aufgaben von Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen im Hinblick auf die digitale operationale Resilienz gemäß der Verordnung (EU) 2022/2554<sup>10</sup>.

---

<sup>9</sup> Leitlinien EBA/GL/2019/02 zu Auslagerungen.

<sup>10</sup> Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

## 4.2 Sorgfaltspflicht und Überprüfungsmaßnahmen für die Analyse von Warnmeldungen

### 4.2.1 Strategien und Verfahren für das Management und die Analyse von Warnmeldungen

31. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten über Strategien und Verfahren zur Untersuchung von Warnmeldungen im Zusammenhang mit restriktiven Maßnahmen verfügen. Diese Strategien und Verfahren sollten es den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen ermöglichen, zu bestätigen, ob es sich bei einer Warnmeldung um einen echt-positiven Treffer handelt, und die erforderlichen Maßnahmen zur Einhaltung der geltenden restriktiven Maßnahme festzulegen.
32. Diese Strategien und Verfahren sollten Folgendes umfassen:
  - a. Maßnahmen zur Einleitung einer unverzüglichen Untersuchung aller potenziellen Treffer für jeden Geldtransfer oder Kryptowertetransfer;
  - b. Regeln für die Dokumentation von Entscheidungen über Warnmeldungen, die mit der allgemeinen Strategie für das Führen von Aufzeichnungen der Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen vereinbar sind;
  - c. Maßnahmen zur Einhaltung von Abschnitt 4.2.2 dieser Leitlinien;
  - d. verschiedene Überprüfungsebenen, die entsprechend der Risikobewertung in Bezug auf restriktive Maßnahmen anzuwenden sind, wobei in Fällen mit höherem Risiko mindestens eine Überprüfung durch zwei Personen durchzuführen ist.

### 4.2.2 Sorgfaltspflicht bei der Analyse der Warnmeldungen

33. Die vom Überprüfungssystem generierte Warnmeldung sollte die Art der betreffenden restriktiven Maßnahme anzeigen. Warnmeldungen sollten von Mitarbeitern analysiert werden, die über das erforderliche Fachwissen verfügen und ausreichend geschult sind<sup>11</sup>.
34. Wenn Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen Zweifel an der Richtigkeit eines Treffers haben, sollten sie zusätzliche Informationen, über die sie verfügen und/oder die sie erhalten, nutzen, um die Analyse der Warnmeldungen zu unterstützen, sofern solche Informationen verfügbar sind, wie z. B.:
  - a. Daten zur Identifizierung einer natürlichen oder juristischen Person, Organisation oder Einrichtung, die in der Überprüfungsphase nicht verwendet wurden;
  - b. Informationen über den Wohnsitz einer natürlichen Person und Informationen über den Sitz oder den eingetragenen Geschäftssitz einer juristischen Person, Organisation oder Einrichtung, die in der Überprüfungsphase nicht verwendet wurden;

---

<sup>11</sup> Siehe Abschnitt 4.4 der Leitlinien zu internen Strategien, Verfahren und Kontrollen, die die Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten sicherstellen.

- c. Informationen über Staatsangehörigkeit und Staatsbürgerschaft natürlicher Personen, die in der Überprüfungsphase nicht verwendet wurden;
  - d. Vertretungs-, Leitungs- und Organisationsstruktur juristischer Personen, die in der Überprüfungsphase nicht verwendet wurden;
  - e. Kontaktdaten, die in der Überprüfungsphase nicht verwendet wurden.
35. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, wie in Fällen zu verfahren ist, in denen nach einer zusätzlichen Sorgfaltsprüfung nicht eindeutig festgestellt werden kann, ob es sich bei einem Treffer um einen echt-positiven Treffer, einen falsch-positiven Treffer oder eine Namensgleichheit handelt. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten davon absehen, Finanzdienstleistungen für eine an einem Transfer beteiligte Partei zu erbringen, bevor sie eine fundierte Entscheidung getroffen haben.

#### **4.2.3 Beurteilung, ob sich eine Organisation im Eigentum oder unter der Kontrolle einer benannten Person befindet**

36. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, wie sie beurteilen, ob sich eine juristische Person oder ein Unternehmen im Eigentum oder unter der Kontrolle einer benannten Person oder Organisation befindet.
37. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten
- a. die in den Sanktionsleitlinien des Rates<sup>12</sup> und in Abschnitt VIII der bewährten Praktiken des Rates<sup>13</sup> aufgeführten Kriterien für die Beurteilung, ob sich eine juristische Person im Eigentum oder unter der Kontrolle einer anderen Person oder Organisation befindet, anwenden;
  - b. die Kriterien für die Identifizierung eines wirtschaftlichen Eigentümers gemäß den geltenden Rechtsvorschriften anwenden<sup>14</sup>;
  - c. verfügbare öffentliche Informationsquellen nutzen, wie z. B. Register der sich im Besitz befindlichen und kontrollierten Organisationen und Register der wirtschaftlichen Eigentümer.
38. Ist die Bewertung nach wie vor nicht schlüssig, sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen eine Zusammenarbeit mit der für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörde in Erwägung ziehen. Die Verantwortung für die Einhaltung der restriktiven Maßnahmen liegt letztlich bei den Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen.

---

<sup>12</sup> <https://data.consilium.europa.eu/doc/document/ST-11618-2024-INIT/en/pdf>, Brüssel, 2. Juli 2024, 11618/24 (Aktualisierung).

<sup>13</sup> „Aktualisierung der bewährten Praktiken der EU für die wirksame Umsetzung restriktiver Maßnahmen“ (Dok. 11623/24).

<sup>14</sup> Artikel 3 Nummer 6 der Richtlinie (EU) 2015/849.

#### **4.2.4 Kontrollen und Sorgfaltspflichtmaßnahmen zur Einhaltung sektorspezifischer restriktiver Maßnahmen**

39. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten bei der Festlegung der Arten von Kontrollen, die sie zur Einhaltung restriktiver Maßnahmen anwenden, die Risikobewertung in Bezug auf restriktive Maßnahmen berücksichtigen. In diesem Zusammenhang sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen festlegen, welche verfügbaren Informationen im Zusammenhang mit einer Transaktion zu überprüfen sind.
40. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten insbesondere auf sektorspezifische restriktive Maßnahmen achten, die sich auf eine bestimmte Rechtsordnung oder ein bestimmtes Gebiet beziehen. Im Rahmen dieser restriktiven Maßnahmen sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen alle zugrunde liegenden Informationen im Zusammenhang mit Geldtransfers oder Kryptowertetransfers in die oder aus den betreffenden Rechtsordnungen oder Gebieten oder mit Geldtransfers oder Kryptowertetransfers überprüfen, die von Kunden veranlasst werden, von denen bekannt ist, dass sie in der betreffenden Rechtsordnung oder dem betreffenden Gebiet Geschäfte tätigen. Soweit verfügbar, sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen Folgendes überprüfen:
- a. Informationen über Staatsangehörigkeit(en), Geburtsort;
  - b. Informationen über den gewöhnlichen Aufenthaltsort oder den Hauptgeschäftssitz über andere Anschriften im Einklang mit der Risikobewertung in Bezug auf restriktive Maßnahmen;
  - c. Informationen über das Land, in das oder aus dem der Geldtransfer erfolgt, und über den Ort, an dem der Geldtransfer ausgeführt wird;
  - d. Zweck des Geldtransfers oder des Transfers von Kryptowerten und weitere Freitextfelder, die entsprechend der Risikobewertung in Bezug auf restriktive Maßnahmen weitere Informationen über die Waren, Schiffe, Bestimmungs- oder Herkunftsländer der Waren, für die die Zahlung geleistet wird, enthalten.
41. Wenn die Risikobewertung in Bezug auf restriktive Maßnahmen dies rechtfertigt, sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen in Erwägung ziehen, in ihre Überprüfungssysteme Instrumente zur Geo-Lokalisierung und zur Erkennung der Nutzung von Proxy-Diensten aufzunehmen, um IP-Adressen aus einem Land, für das aufgrund der Lage restriktive Maßnahmen gelten, zu ermitteln und daran zu hindern, auf die Website und die Dienste des Zahlungsdienstleisters oder Anbieters von Krypto-Dienstleistungen zuzugreifen, um eine Tätigkeit auszuüben, die nach den Regelungen bezogen auf die restriktiven Maßnahmen verboten ist.
42. Entsprechend ihrer Risikobewertung in Bezug auf restriktive Maßnahmen können Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen die Anwendung spezieller Kontrollen in Erwägung ziehen, wie z. B.:

- a. bei der Aufnahme von Geschäftsbeziehungen Einholung relevanter Informationen über die Art der Geschäftstätigkeit von dem Kunden und die Länder, in denen der Kunde tätig ist;
  - b. Anforderung zusätzlicher Informationen vom Kunden, wie z. B. eine Beschreibung von Gütern mit doppeltem Verwendungszweck oder von Gütern, die sektorspezifischen restriktiven Maßnahmen unterliegen, Informationen über die entsprechende Genehmigung für den Handel mit Gütern mit doppeltem Verwendungszweck, das Ursprungsland der Güter, Informationen über den Endverwender der Güter;
  - c. Anforderung genauerer Informationen vom Kunden über den Zweck eines Geldtransfers oder Kryptowertetransfers;
  - d. Verwendung der folgenden Daten: Schiffsregister, Grundbucheintragungen und andere öffentlich zugängliche Datensätze (sofern verfügbar).
43. Wenn Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen Funktionen zum automatischen Auslesen von Informationen aus Dokumenten im Zusammenhang mit dem Geldtransfer oder dem Transfer von Kryptowerten verwenden, wie z. B. OCR-Algorithmen oder maschinenlesbare Zonenprüfungen, sollten sie die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass diese Instrumente die Informationen korrekt und einheitlich erfassen.

#### **4.2.5 Sorgfaltspflicht zur Aufdeckung von Versuchen, restriktive Maßnahmen zu umgehen**

44. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten sich über Typologien und Trends bei der Umgehung restriktiver Maßnahmen auf dem Laufenden halten. Zu den einschlägigen Informationsquellen, auf die sich Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen stets stützen sollten, gehören zumindest Berichte, die von folgenden Stellen veröffentlicht werden:
- a. die für die Durchführung von restriktiven Maßnahmen zuständigen nationalen Behörden<sup>15</sup> und/oder die nationalen Aufsichtsbehörden;
  - b. zentrale Meldestellen für Finanztransaktionsuntersuchungen und Strafverfolgungsbehörden;
  - c. einschlägige öffentlich-private Partnerschaften auf nationaler oder EU-Ebene;
  - d. EU-Behörden<sup>16</sup>.
45. Die Strategien und Verfahren zur Erfüllung der Sorgfaltspflicht sollten es Zahlungsdienstleistern und Anbietern von Krypto-Dienstleistungen erlauben, mögliche Versuche zur Umgehung restriktiver Maßnahmen zu erkennen, wie etwa Versuche:
- a. Informationen in Zahlungsnachrichten wegzulassen, zu löschen oder zu ändern;

---

<sup>15</sup> [https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources\\_en#contact](https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact).

<sup>16</sup> Siehe beispielsweise [https://finance.ec.europa.eu/news/sanctions-commission-publishes-guidance-help-european-operators-assess-sanctions-circumvention-risks-2023-09-07\\_en](https://finance.ec.europa.eu/news/sanctions-commission-publishes-guidance-help-european-operators-assess-sanctions-circumvention-risks-2023-09-07_en).

- b. Transfers über Personen abzuwickeln, die mit einem Kunden in Verbindung stehen, für den restriktive Maßnahmen gelten;
  - c. Geldtransfers oder Transfers von Kryptowerten so zu strukturieren, dass die Beteiligung einer benannten Partei verschleiert wird;
  - d. das wirtschaftliche Eigentum oder die Kontrolle von Vermögenswerten zu verschleiern;
  - e. gefälschte oder betrügerische Hintergrunddokumente für Geldtransfers oder Transfers von Kryptowerten zu verwenden.
46. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen, bei denen ein hohes Risiko hinsichtlich der Umgehung restriktiver Maßnahmen besteht, sollten auch eine aggregierte Analyse der Zahlungsströme in oder aus Ländern, die restriktiven Maßnahmen unterliegen, sowie in und aus Ländern, die bekanntermaßen zur Umgehung restriktiver Maßnahmen genutzt werden, in Erwägung ziehen.

## 4.3 Einfrieren von Geldern und Meldungen

### 4.3.1 Aussetzung der Ausführung von Geldtransfers und Einfrieren von Geldern

47. Die Zahlungsdienstleister sollten über Strategien und Verfahren verfügen, um Transaktionen unverzüglich auszusetzen, die eine Warnmeldung hinsichtlich eines möglichen Treffers bezüglich einer benannten Person oder Organisation oder einer Person, die sich im Eigentum, Besitz oder unter der Kontrolle einer benannten Person oder Organisation befindet oder deren wirtschaftlicher Eigentümer eine benannte Person ist, auslösen.
48. Bestätigt die interne Analyse einer solchen Warnmeldung durch den Zahlungsdienstleister, dass es sich bei dem möglichen Treffer um die benannte Person oder Organisation handelt oder dass sie sich im Eigentum, Besitz oder unter der Kontrolle einer benannten Person oder Organisation befindet oder dass ihr wirtschaftlicher Eigentümer eine benannte Person ist, so sollte der Zahlungsdienstleister unverzüglich:
- a. die entsprechenden Mittel einfrieren;
  - b. die Ausführung von Geldtransfers, die gegen restriktive Maßnahmen verstoßen würden, einstellen.

### 4.3.2 Einfrieren des Transfers von Kryptowerten

49. Die Anbieter von Krypto-Dienstleistungen sollten über Strategien und Verfahren verfügen, um für den Fall, dass eine interne Analyse einer Warnmeldung bestätigt, dass es sich bei dem möglichen Treffer um die benannte Person oder Organisation handelt oder dass sie sich im Eigentum oder Besitz einer benannten Person oder Organisation befindet oder von dieser kontrolliert wird oder dass es sich bei dem wirtschaftlichen Eigentümer um eine benannte Person handelt, die Gelder unverzüglich einzufrieren und auf einem Verwahrkonto zu sperren, bis der jeweilige Anbieter von Krypto-Dienstleistungen von der für die Durchführung restriktiver Maßnahmen zuständigen nationalen Behörde darüber unterrichtet wird, wie mit



diesen Geldern zu verfahren ist. Die Verantwortung für die Einhaltung der restriktiven Maßnahmen liegt letztlich beim Anbieter von Krypto-Dienstleistungen.

#### 4.3.3 Meldungen

50. Im Einklang mit den geltenden Anforderungen auf Unionsebene und auf nationaler Ebene sollten Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen über klare Verfahren verfügen, um der für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörde und/oder der zuständigen Aufsichtsbehörde unverzüglich oder innerhalb einer bestimmten Frist Bericht zu erstatten über:
- a. alle Maßnahmen, die für einen bestimmten Transfer im Zusammenhang mit einer restriktiven Maßnahme ergriffen werden;
  - b. die Feststellung eines Verstoßes gegen restriktive Maßnahmen und
  - c. die Ausführung von Geldtransfers oder Kryptowertetransfers, die gegen eine geltende restriktive Maßnahme verstoßen, indem sie Informationen über die Umstände, z. B. eine Störung in der Funktionsweise des Überprüfungssystems im Zusammenhang mit einem solchen Transfer, bereitstellen.
51. Bei Verdacht auf eine mögliche Umgehung restriktiver Maßnahmen oder der Feststellung eines versuchten Geldtransfers oder Kryptowertetransfers durch oder an eine natürliche Person, juristische Person, Organisation oder Einrichtung sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen:
- a. dies der für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörde melden, sofern dies in einer EU-Verordnung über restriktive Maßnahmen ausdrücklich vorgesehen ist;
  - b. die verdächtige Transaktion melden, wenn dies nach den geltenden Rechtsvorschriften erforderlich ist.

#### 4.3.4 Verfahren für Ausnahmen oder bei der Aufhebung restriktiver Maßnahmen

52. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten über Strategien und Verfahren verfügen, um festzustellen, ob Ausnahmeregelungen, Genehmigungsregelungen oder Freistellungen anwendbar sind, und, falls dies der Fall ist, wie zu verfahren ist, um die Einhaltung des geltenden Unionsrechts oder des geltenden nationalen Rechts zu gewährleisten. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten in ihren Strategien und Verfahren festlegen, welche Informationen sie Kunden, die eine Ausnahmeregelung für die Verwendung ihrer eingefrorenen Gelder beantragen möchten, zur Verfügung stellen werden, sofern eine solche Ausnahmeregelung nach dem geltenden Rechtsrahmen zulässig ist. Diese Informationen sollten Angaben über die Rechte des Kunden in diesem Fall enthalten.

53. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten über Strategien und Verfahren verfügen, wie mit Geldern und Kryptowerten umzugehen ist, die Gegenstand spezieller restriktiver Maßnahmen sind, wenn diese Maßnahmen aufgehoben werden.

#### 4.4 Sicherstellung der fortlaufenden Wirksamkeit der Strategien, Verfahren und Systeme zur Überprüfung restriktiver Maßnahmen

54. Um wirksam zu sein, sollten die Strategien, Verfahren und Systeme zur Überprüfung restriktiver Maßnahmen eines Zahlungsdienstleisters oder Anbieters von Krypto-Dienstleistungen Folgendes ermöglichen:
- a. positive Treffer zuverlässig zu erkennen;
  - b. bei Bestätigung eines positiven Treffers unverzüglich die Ausführung eines Geldtransfers auszusetzen, eingehende Transfers zu sperren und sie auf einem Verwahrkonto zu hinterlegen, die betreffenden Gelder oder Kryptowerte unverzüglich einzufrieren und diese Maßnahmen der für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörde zwecks weiterer Anweisungen zu melden;
  - c. die eingefrorenen Vermögenswerte den für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörden und/oder der zuständigen Aufsichtsbehörde gemäß den geltenden Rechtsvorschriften unverzüglich oder innerhalb der im geltenden Unionsrecht oder im nationalen Recht festgesetzten Fristen zu melden;
  - d. der für die Umsetzung restriktiver Maßnahmen zuständigen nationalen Behörde oder der nationalen zentralen Meldestelle für Finanztransaktionsuntersuchungen jeden Verdacht auf Umgehung oder versuchte Umgehung restriktiver Maßnahmen zu melden, sofern dies nach den geltenden Rechtsvorschriften erforderlich ist.
55. Die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten die Konfiguration ihres Überprüfungssystems regelmäßig testen, um festzustellen, ob das Überprüfungssystem vor dem Hintergrund der Risikobewertung in Bezug auf restriktive Maßnahmen der Zahlungsdienstleister oder Anbieter von Krypto-Dienstleistungen weiterhin angemessen ist und wirksam ist. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten die Häufigkeit der Kontrollen auf der Grundlage der Risikobewertung in Bezug auf restriktive Maßnahmen festlegen und sie in ihren Strategien und Verfahren dokumentieren.
56. Bei der Kontrolle ihres Überprüfungssystems sollten die Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen
- a. die Kalibrierung des Überprüfungssystems gemäß Abschnitt 4.1.6 testen;
  - b. die Genauigkeit der Listenverwaltung unter Anwendung der geltenden und aktuellen restriktiven Maßnahmen bewerten;
  - c. beurteilen, ob alle Kunden, Geldtransfers und Kryptowertetransfers bei Bedarf überprüft werden;

- d. die Angemessenheit und Relevanz der im Überprüfungssystem verwendeten Informationsfelder bewerten, wie z. B. des Umfangs der in das Überprüfungssystem eingegebenen Geldtransfers oder Kryptowertetransfers;
  - e. die Rechtzeitigkeit der automatischen Aussetzung von Vorgängen bewerten;
  - f. bewerten, ob die Prozesse und Ressourcen, die für die Analyse von Warnmeldungen zur Verfügung stehen, eine rasche Meldung von echt-positiven Treffern ermöglichen.
57. Zahlungsdienstleister und Anbieter von Krypto-Dienstleistungen sollten dem Leitungsorgan wesentliche Schwachstellen oder Mängel des Überprüfungssystems melden und unverzüglich Korrekturmaßnahmen ergreifen.