Blockchain Bundesverband e. V.

Berlin, 19.11.2026

Stellungnahme zum GwBG

Blockchain Bundesverband e.V. (Bundesblock)
Interessenvertretung für Blockchain und DLT in Deutschland
Mühlenstr. 8a
14167 Berlin

Bundesministerium der Finanzen
Referat VII A 5
Wilhelmstraße 97
10117 Berlin

Per E-Mail an VIIA5@bmf.bund.de

GZ: VII A 5 - WK 5023/01042/016/004
DOK: COO.7005.100.4.15886746

Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der Sechsten EU-Geldwäscherichtlinie und zur Stärkung der Geldwäscheprävention (Geldwäschebekämpfungsgesetz – GwBG)

Sehr geehrte Damen und Herren,

der Blockchain Bundesverband e.V. vertritt Unternehmen aus den Bereichen Kryptowerte-Dienstleistungen, tokenisierte Finanzmärkte und Blockchain-Infrastruktur. Wir bedanken uns für die Gelegenheit, zum Referentenentwurf vom 28.10.2026 Stellung zu nehmen. Unsere Anmerkungen beschränken sich bewusst auf Regelungen mit Bezug zu Kryptowerten und Anbietern von Kryptowerte-Dienstleistungen (CASPs); eine Bewertung sämtlicher Vorschriften ist damit nicht verbunden.

Kurzfassung: Der Blockchain Bundesverband unterstützt die 1:1-Umsetzung des EU-Geldwäschepakets ausdrücklich. Handlungsbedarf sehen wir dort, wo der Entwurf neue operative Pflichten für CASPs begründet: beim Kontenabruf für Kryptowertekonten, bei Anordnungen der FIU und bei der Aufsicht über passportierte Anbieter. Hier fordern wir klare Begriffe, eine Haftungsfreistellung und praxisgerechte Übergangsregelungen.

Aufbau: Teil A enthält unsere grundsätzliche Einordnung und Kernforderungen. Teil B enthält Anmerkungen und Formulierungsvorschläge zu einzelnen Vorschriften in der Reihenfolge des Referentenentwurfs. Normzitate mit „-E“ beziehen sich auf den Entwurf; AMLR bezeichnet die Verordnung (EU) 2024/1624, AMLD6 die Richtlinie (EU) 2024/1640, TFR die Verordnung (EU) 2023/1113 und MiCAR die Verordnung (EU) 2023/1114.

Mit einer Veröffentlichung dieser Stellungnahme auf der Internetseite des Bundesministeriums der Finanzen sind wir einverstanden.

Teil A: Grundsätzliche Anmerkungen

I. Einordnung

Unsere Linie: Harmonisierung statt nationaler Sonderwege. CASPs unterliegen mit MiCAR, TFR und AMLR bereits einem vollharmonisierten europäischen Rahmen. Da CASPs ihren Herkunftsmitgliedstaat frei wählen und ihre Lizenz EU-weit passportieren können, wirkt jede nationale Zusatzpflicht unmittelbar als Standortnachteil für Deutschland.

Aus Sicht des Blockchain Bundesverbands geht der Entwurf daher in die richtige Richtung. Wir begrüßen insbesondere:

- **Wegfall der ART-Verpflichtung:** Emittenten vermögenswertereferenzierter Token (ARTs) werden nicht mehr national weiterverpflichtet.
- **Keine Sonderregeln zu Self-Custody:** Der Entwurf verzichtet auf nationale Vorgaben zu selbstverwalteten Wallets neben Art. 14 Abs. 5 und Art. 16 Abs. 2 TFR.
- **Fokussierte Meldepflicht:** Die Meldepflicht konzentriert sich auf besonders geldwäscherelevante Vortaten.
- **Keine Doppelregistrierung:** Bereits lizenzierte Verpflichtete müssen sich nicht zusätzlich bei der Aufsicht registrieren (§ 6 Abs. 2 Satz 2 GwBG-E).

Viele operative Details hängen allerdings von noch ausstehenden RTS und Durchführungsrechtsakten ab. Das Gesetz sollte deshalb klare Grundbegriffe setzen und ausreichende Übergangsfristen vorsehen; es darf keine Unsicherheiten in die Aufsichtspraxis verlagern.

II. Unsere Kernforderungen

1. **Kontenabruf (§ 24c KWG-E, § 45a KMAG-E):** Wir fordern eine gesetzliche Definition der „Zuordnungsnummern“, einen präzisen Anwendungsbereich und eine Übergangspraxis der Aufsicht für die erstmalige technische Anbindung.
2. **Passporting (§§ 79, 80 GwBG-E):** Die über Art. 38 Abs. 1 AMLD6 hinausgehende Erfassung des grenzüberschreitenden Dienstleistungsverkehrs in § 79 Abs. 1 ist von der Richtlinie nicht gedeckt und sollte gestrichen werden; das reine Online-Angebot nach Art. 65 MiCAR darf keine Gastlandaufsicht begründen. Die Kontaktstellenpflicht sollte ausdrücklich an die RTS-Kriterien anknüpfen.
3. **FIU-Anordnungen (§§ 51, 52 GwBG-E):** Wir fordern eine klarstellende Haftungsfreistellung der Verpflichteten, eine Befristung von Überwachungsanordnungen mit begründeter Verlängerung und Klarheit zur Reichweite bei Kryptowerten.
4. **Datenanalyse und Meldewesen der FIU (§§ 65, 72 GwBG-E):** Wir fordern eine Klarstellung, dass Transaktionsdaten öffentlicher Blockchains in automatisierte Analysen einbezogen werden dürfen, sowie eine Anhörung der Verpflichteten vor der Festlegung von Meldetypologien.
5. **Verpflichtetenkreis (§ 3 Abs. 1 Nr. 3 GwBG-E):** Wir empfehlen, die Risikobewertung zu veröffentlichen und eine nur teilweise Anwendung der AMLR zu prüfen.
6. **Immobilien (§ 9 GwBG-E):** Wir regen an, Transfers über MiCAR-lizenzierte CASPs mit vollständigen Travel-Rule-Daten nicht länger mit Bargeld gleichzusetzen.
7. **TFR-Bußgelder (§ 118 GwBG-E):** Wir empfehlen einen abschließenden, bestimmten Bußgeldkatalog und den Ausschluss paralleler Sanktionen nach KMAG.
8. **Erfüllungsaufwand:** Der Aufwand der CASPs für Kontenabruf und neue Datenformate sollte gesondert ausgewiesen werden.

Teil B: Anmerkungen und Formulierungsvorschläge zu einzelnen Vorschriften

B1. § 3 Abs. 1 Nr. 3 GwBG-E: Nationale Erweiterung des Verpflichtetenkreises

Institute mit qualifiziertem Kryptoverwahrgeschäft (§ 1 Abs. 1a Satz 2 Nr. 6 KWG) oder Kryptowertpapierregisterführung (Nr. 8) sollen gestützt auf Art. 3 Abs. 7 AMLD6 Verpflichtete bleiben, und zwar unter vollständiger Anwendung der AMLR (§ 3 Abs. 2).

Fehlende Transparenz. Die Weiterverpflichtung stützt sich nach der Begründung auf eine Risikoeinschätzung der BaFin, die nicht veröffentlicht ist. Betroffene Institute können die Annahmen daher nicht nachvollziehen.

Registerführung ist Infrastruktur. Die Registerführung nach eWpG kommt ohne eigene Kundengelder und ohne Zahlungsfunktion aus. Vertrieben werden Kryptowertpapiere regelmäßig über bereits verpflichtete Verwahrer oder Banken. Hinzu kommt: Andere Mitgliedstaaten kennen vergleichbare Registerführer nicht, sodass die Vollverpflichtung das deutsche eWpG-Modell im Wettbewerb schwächt. Art. 3 Abs. 7 AMLD6 erlaubt ausdrücklich, nur Teile der AMLR anzuwenden.

Vorschlag: Wir empfehlen,

- eine Zusammenfassung der Risikobewertung zu veröffentlichen (vgl. § 7 Abs. 5 GwBG-E), spätestens zusammen mit der Begründung, die nach Art. 3 Abs. 7 Unterabsatz 2 AMLD6 bis zum 10. Januar 2028 der Kommission vorzulegen ist,
- für die Kryptowertpapierregisterführung auf die Weiterverpflichtung zu verzichten oder sie auf Meldepflicht und grundlegende Sorgfaltspflichten zu beschränken, soweit keine eigenen Kundenbeziehungen zu den Inhabern bestehen,
- Doppelpflichten auszuschließen, wenn ein Institut zugleich CASP nach MiCAR ist.

B2. § 9 GwBG-E: Kryptowerte im Barzahlungsverbot bei Immobilien

§ 9 führt § 16a GwG fort: Kryptowerte bleiben als Gegenleistung beim Immobilienerwerb neben Bargeld, Gold, Platin und Edelsteinen unzulässig.

Kryptowerte sind kein Bargeld. Seit Geltung von MiCAR und TFR ist diese Gleichstellung nicht mehr sachgerecht. Ein Transfer zwischen zwei lizenzierten CASPs ist vollständig rückverfolgbar: Die Travel Rule übermittelt Auftraggeber- und Begünstigtendaten, beide Seiten unterliegen der AMLR, und die Transaktion ist dauerhaft on-chain dokumentiert.

Ungleichbehandlung von E-Geld-Token. E-Geld-Token sind Kryptowerte im Sinne des § 9 (§ 2 Abs. 1 GwBG-E i. V. m. Art. 2 Abs. 1 Nr. 7 AMLR); die dort in Bezug genommene Ausnahme für Gelder nach Art. 2 Abs. 4 MiCAR gilt für E-Geld-Token gerade nicht. Sie fallen damit unter das Verbot, obwohl sie nach Art. 48 Abs. 2 MiCAR als E-Geld gelten und § 9 E-Geld nicht nennt. Für diese Ungleichbehandlung gibt es keinen sachlichen Grund; sie behindert unnötig den Einsatz tokenisierter Zahlungsformen.

Vorschlag: Wir regen an, Kryptowerte vom Verbot auszunehmen, wenn die Gegenleistung zwischen Kryptowertekonten bei MiCAR-lizenzierten CASPs mit vollständigen Angaben nach Art. 14 TFR übertragen wird. Bestätigungen solcher CASPs sollten in § 9 Abs. 2 Satz 2 den Zahlungsbestätigungen von Kreditinstituten gleichgestellt werden. Unabhängig davon sind E-Geld-Token, die nach Art. 48 Abs. 2 MiCAR als E-Geld gelten, vom Verbot auszunehmen und insoweit wie E-Geld zu behandeln.

B3. §§ 51, 52 GwBG-E: Sofortmaßnahmen und Überwachungsanordnungen

Die FIU kann künftig die Nutzung von Kryptowertekonten bis zu fünf Werktage aussetzen (§ 51 Abs. 2), Transaktionen bis zu zehn Werktage anhalten (§ 51 Abs. 1) und die Überwachung von Kryptowertekonten „für die Dauer eines von ihr festgelegten Zeitraums“ anordnen (§ 52). Für die Sofortmaßnahmen nach § 51 Abs. 1 und 2 haftet sie nicht (§ 51 Abs. 8).

Volatilität und Haftung. Der Blockchain Bundesverband unterstützt wirksame Eingriffsbefugnisse. Bei Kryptowerten führen Sperren wegen der Kursvolatilität aber schnell zu erheblichen Vermögenseinbußen. Da die FIU nicht haftet, drohen sich Ansprüche faktisch gegen den Verpflichteten zu richten, der lediglich die Anordnung befolgt. Insbesondere im Falle einer nichtigen Anordnung könnten sich reale Haftungsrisiken ergeben.

Reichweite bei Self-Custody. CASPs können nur Bestände unter eigener Verfügungsgewalt sperren, nicht aber Kryptowerte in selbstverwalteten Wallets ihrer Kunden.

Unbefristete Überwachung. Allein die FIU legt die Dauer der Überwachungsanordnung fest; eine Befristung oder regelmäßige Überprüfung sieht § 52 nicht vor.

Vorschlag: Wir fordern eine Haftungsfreistellung der Verpflichteten.

Formulierungsvorschlag für § 51 Abs. 8 (Satz 2 und 3 neu) GwBG-E:

„Ein Verpflichteter, der eine Anordnung nach den Absätzen 1 und 2 oder nach § 52 befolgt, haftet hierfür gegenüber dem Kunden oder Dritten nicht, es sei denn, er handelt vorsätzlich oder grob fahrlässig. Dies gilt auch, wenn die Anordnung rechtswidrig oder nichtig ist; eine Pflicht des Verpflichteten zur Prüfung der Rechtmäßigkeit der Anordnung besteht nicht.“

In der Begründung sollte klargestellt werden, dass sich Anordnungen nur auf verwahrte oder kontrollierte Bestände beziehen und keine Pflicht zur Veräußerung oder Umschichtung begründen. § 52 Abs. 1 sollte vorsehen, dass die FIU die Überwachung zunächst befristet (etwa auf drei Monate) anordnet und eine Verlängerung jeweils begründet. Das bleibt im Rahmen von Art. 25 AMLD6, der die Festlegung des Zeitraums der FIU überlässt. Eine solche Befristung entspricht zudem der Systematik der Richtlinie, die für Aussetzungen nach Art. 24 AMLD6 ebenfalls feste Fristen und Rechtsschutz vorsieht. Die Übermittlung der Überwachungsergebnisse an die FIU sollte über goAML erfolgen.

B4. §§ 65, 70, 72 GwBG-E: Datenanalyse und Meldewesen der FIU

Die FIU darf in automatisierten Analysen Kontokennungen von Kryptowertekonten und Adressen selbstverwalteter Wallets verarbeiten (§ 65 Abs. 5 Nr. 15). Personenbezogene Daten aus allgemein zugänglichen Quellen dürfen dabei nicht automatisiert einbezogen werden. Nach § 72 Abs. 2 kann die FIU Transaktionen beschreiben, die stets zu melden sind.

Blockchain-Analyse. Transaktionsdaten öffentlicher Blockchains sind „allgemein zugänglich“. Nach dem Wortlaut von § 65 Abs. 5 dürfte die FIU sie daher nicht automatisiert analysieren. Damit wäre ausgerechnet die Blockchain-Analyse ausgeschlossen, also das wichtigste Werkzeug, um Kryptowerte nachzuverfolgen. Das kann nicht gewollt sein. Der Gesetzgeber sollte Blockchain-Daten deshalb ausdrücklich einbeziehen. Für andere öffentlich zugängliche, personenbezogene Daten, etwa aus sozialen Medien, sollte der Ausschluss dagegen bestehen bleiben.

Gefahr defensiver Massenmeldungen. Pauschale Typologien nach § 72 Abs. 2, etwa jede Transaktion mit Bezug zu Mixern oder Self-Custody-Wallets, würden das Ziel einer fokussierten Meldepflicht konterkarieren.

Vorschlag: Wir empfehlen,

- in § 65 Abs. 5 klarzustellen, dass Transaktionsdaten öffentlicher Distributed Ledger in automatisierte Analysen einbezogen werden dürfen; eine automatisierte Verknüpfung mit sonstigen personenbezogenen Daten aus allgemein zugänglichen Quellen (z. B. soziale Medien) sollte ausgeschlossen bleiben,
- in § 72 Abs. 2 vorzusehen, dass die betroffenen Verpflichteten und ihre Verbände vor der Festlegung von Typologien angehört und die Typologien veröffentlicht werden; zudem sollte von § 72 Abs. 2 Satz 2 Gebrauch gemacht werden, um auch Konstellationen zu beschreiben, die nicht meldepflichtig sind (etwa Transfers an oder von selbst gehosteten Adressen, deren Kontrolle durch den Kunden nach Art. 14 Abs. 5, Art. 16 Abs. 2 TFR festgestellt wurde),
- die Rückmeldung nach § 70 Abs. 2 auch sektorspezifisch für CASPs auszuweisen, etwa zu Kryptotypologien und zur Qualität von Wallet- und Transaktions-Hash-Angaben.

B5. §§ 79, 80 GwBG-E: Aufsicht über passportierte CASPs und zentrale Kontaktstelle

Die BaFin soll CASPs aus anderen Mitgliedstaaten beaufsichtigen, die im Inland „über andere Arten von Infrastruktur“ tätig sind (§ 79 Abs. 1 Nr. 3). Diese CASPs „müssen“ eine zentrale Kontaktstelle im Inland benennen (§ 80 Abs. 1).

Passporting nicht aushebeln. Die meisten CASPs bedienen deutsche Kunden ausschließlich online über den MiCAR-Pass (Art. 65 MiCAR), ohne Personal oder Vertriebspartner im Inland. Gälte bereits die App oder Website als „Infrastruktur“, entstünde

eine geldwäscherechtliche Gastlandaufsicht über nahezu jeden passportierten CASP. Das widerspräche dem Herkunftslandprinzip der MiCAR und führte zu Doppelaufsicht. § 79 Abs. 1 geht dabei über Art. 38 Abs. 1 AMLD6 hinaus: Die Richtlinie nennt nur Agenten, Distributoren und andere Arten von Infrastruktur, § 79 Abs. 1 erfasst zusätzlich ausdrücklich Tätigkeiten „im Wege des grenzüberschreitenden Dienstleistungsverkehrs“.

Wortlaut und Begründung fallen auseinander. § 80 Abs. 1 ist als unbedingte Pflicht formuliert; die Bindung an die RTS-Kriterien ergibt sich nur mittelbar aus Abs. 3. Die Begründung spricht dagegen von Infrastruktur „über Agenten, Distributoren oder Vertriebspartner“.

Vorschlag: Wir fordern eine ausdrückliche Bindung an die RTS-Kriterien und eine Klarstellung zum reinen Online-Angebot. Bis zum Erlass des RTS sollte keine Benennungspflicht entstehen. Der RTS nach Art. 41 Abs. 2 AMLD6 ist bislang nicht erlassen; die geltende Delegierte Verordnung (EU) 2018/1108 betrifft nur E-Geld-Emittenten und Zahlungsdienstleister, ihre Erweiterung auf CASPs ist noch nicht im Amtsblatt veröffentlicht. In § 79 Abs. 1 sollte die über Art. 38 Abs. 1 AMLD6 hinausgehende Angabe „im Wege des grenzüberschreitenden Dienstleistungsverkehrs“ gestrichen werden.

Formulierungsvorschlag für § 79 Abs. 1 (Satz 2 neu) GwBG-E:

„Das Erbringen von Kryptowerte-Dienstleistungen ausschließlich im Wege des grenzüberschreitenden Dienstleistungsverkehrs nach Artikel 65 der Verordnung (EU) 2023/1114 ohne Agenten, Distributoren oder Vertriebspartner im Inland gilt für sich genommen nicht als Tätigkeit über andere Arten von Infrastruktur im Sinne von Satz 1 Nr. 3.“

Formulierungsvorschlag für § 80 Abs. 1 GwBG-E:

„… müssen, sofern die Kriterien des technischen Regulierungsstandards nach Artikel 41 Absatz 2 der Richtlinie (EU) 2024/1640 erfüllt sind, gegenüber der Bundesanstalt für Finanzdienstleistungsaufsicht eine zentrale Kontaktstelle im Inland benennen.“

B6. § 118 GwBG-E: Bußgeldvorschriften zur TFR

§ 118 Abs. 1 Nr. 15 bis 20 ahndet Verstöße von CASPs gegen Art. 14 Abs. 1 bis 3, Art. 17 Abs. 1, Art. 19, 20 und 21 Abs. 1 TFR, mit Geldbußen bis zu 10 Mio. Euro bzw. 10 % des Konzernumsatzes.

Bestimmtheit des Katalogs. Für Geldtransfers sind die Richtigkeitsprüfung (Art. 4 Abs. 4, Art. 7 Abs. 3 TFR), die Erkennungsverfahren des Begünstigten-Dienstleisters (Art. 7 Abs. 1 und 2 TFR) und die Pflichten bei wiederholt fehlenden Angaben (Art. 8 Abs. 2, Art. 12 Abs. 2 TFR) erfasst. Für Kryptowertetransfers fehlen vergleichbare Tatbestände, etwa zur Erkennung fehlender oder unvollständiger Angaben durch den CASP des Begünstigten (Art. 16 TFR). Der Katalog sollte insoweit vervollständigt und abschließend gefasst werden.

Vorschlag: Wir empfehlen, den Katalog um die entsprechenden Pflichten bei Kryptowertetransfers zu ergänzen und parallele Sanktionen nach KMAG für denselben Sachverhalt auszuschließen. Redaktionell regen wir an, in § 118 Abs. 4 und 5 „Artikel 2

Nummer 5“ bzw. „Nummer 6“ durch „Artikel 2 Absatz 1 Nummer 5“ bzw. „Nummer 6“ der AMLR zu ersetzen. Wir empfehlen, in der Begründung zu erläutern, welche Pflichten der TFR bewusst nicht bußgeldbewehrt sind.

B7. Art. 4 und 5 – § 24c KWG-E, § 45a KMAG-E: Kontenabruf für Kryptowertekonten

CASPs, „die für Kunden Kryptowerte verwahren“, müssen künftig ein Dateisystem nach § 24c KWG führen. Die Kontokennung umfasst auch „Zuordnungsnummern, die für die Zuordnung von Kryptowerten zu Kunden genutzt werden“. Über BARIS (§ 24d KWG-E) fließen die Daten auch an Stellen anderer Mitgliedstaaten. Die Einbeziehung als solche ist durch Art. 16 Abs. 3 AMLD6 vorgegeben.

Was sind „Zuordnungsnummern“? Der Begriff ist im Gesetz nicht definiert; die Begründung erläutert nur, dass Zuordnungsnummern zu übermitteln sind, wenn keine gesonderten Kryptowertekonten geführt werden. CASPs halten Kundenbestände regelmäßig in Omnibus-Wallets und vergeben je Kunde wechselnde Einzahlungsadressen. Unklar ist, ob nur die interne Kundenkennung oder auch Blockchain-Adressen einzustellen sind. Letzteres wäre technisch kaum handhabbar und würde öffentlich einsehbare Transaktionshistorien über BARIS EU-weit mit Klardaten verknüpfen. Art. 16 Abs. 3 Buchst. f AMLD6 verlangt für Kryptowertekonten lediglich die einheitliche Kontokennung sowie das Datum der Kontoeröffnung und -schließung; mehr sollte auch das nationale Recht nicht verlangen.

Wer ist erfasst? Der Kreis der Institute in § 45a Abs. 1 KMAG-E („die für Kunden Kryptowerte verwahren“) deckt sich nicht mit dem Begriff des Kryptowertekontos nach Art. 2 Abs. 1 Nr. 24 AMLR, an den § 24c Abs. 1 Satz 1 Nr. 7 KWG-E und die Begründung anknüpfen. Offen ist etwa, ob Handelsplattformen erfasst sind, die Kundenbestände nur kurzfristig halten. Kreditinstitute, die Kryptowerte-Dienstleistungen nach Art. 60 MiCAR erbringen, führen bereits ein Dateisystem; eine doppelte Erfassung sollte ausgeschlossen sein.

Realistische Fristen. CASPs sind bislang nicht an das Kontenabrufverfahren angebunden. Nötig sind Anschluss an das geschlossene Benutzersystem und Hardware nach BaFin-Vorgaben (§ 24c Abs. 7 KWG-E). Ein Start zum 10. Juli 2027 ohne Übergangsfrist ist nicht realistisch, solange die technischen Vorgaben nicht veröffentlicht sind.

Vorschlag: Wir fordern eine gesetzliche Definition der Zuordnungsnummern und die Anknüpfung des Anwendungsbereichs an Art. 2 Abs. 1 Nr. 24 AMLR; Kreditinstitute, die bereits ein Dateisystem führen, sollten Kryptowertekonten dort erfassen können, ohne ein zweites System zu führen. Da Art. 16 AMLD6 ohne Ausnahme bis zum 10. Juli 2027 umzusetzen ist (Art. 78 Abs. 1 AMLD6), sollten die technischen Vorgaben unverzüglich veröffentlicht werden. Für die erstmalige technische Anbindung regen wir eine Übergangspraxis der BaFin an, nach der Verzögerungen, die auf spät veröffentlichte Vorgaben zurückgehen, nicht sanktioniert werden.

Formulierungsvorschlag für § 45a Abs. 1 (Satz 2 neu) KMAG-E:

„Zuordnungsnummern im Sinne des Satzes 1 sind die vom Institut zur internen Zuordnung von Kryptowerten zu einem Kunden vergebenen Kunden- oder Unterkontokennungen; Adressen in einem Distributed Ledger sind nicht zu speichern."

B8. § 45a Abs. 2 KMAG-E, § 24e KWG-E und Art. 15: Weitere Folgeänderungen

Transaktionsdaten für die Strafverfolgung. Die entsprechende Anwendung von § 24e KWG-E auf CASPs ist sachgerecht. Die Formatvorgaben nach Art. 6a Abs. 2 der Richtlinie (EU) 2019/1153 sollten erst nach angemessener Frist ab Erlass des Durchführungsrechtsakts verbindlich werden.

Kryptowerte-Steuertransparenz-Gesetz (KryptoStTG). Die Anpassung der Verweise an Art. 20 AMLR begrüßen wir. Wir regen an, in der Begründung klarzustellen, dass nach der AMLR erhobene Identifizierungsdaten für Zwecke des KryptoStTG ohne erneute Erhebung genutzt werden können.

B9. Weitere Anregungen

- **Erfüllungsaufwand:** Die Darstellung weist keinen Aufwand der CASPs für die Anbindung an das Kontenabrufverfahren (§ 45a KMAG-E i. V. m. § 24c Abs. 7 KWG-E) und für neue Transaktionsdatenformate aus. Wir regen an, diesen Aufwand zu ergänzen; unsere Mitglieder liefern hierzu gern Erfahrungswerte.
- **Partnerschaften für den Informationsaustausch (§ 114 GwBG-E):** Wir begrüßen die Grundlage für Partnerschaften nach Art. 75 AMLR. Gerade bei Anlagebetrug und „Pig Butchering" ermöglicht der schnelle Austausch von Wallet-Adressen zwischen CASPs, Banken und Behörden die Sicherung von Vermögenswerten.
- **Ressourcen von FIU und Aufsicht (§ 92 GwBG-E):** Die Wirksamkeit der neuen Befugnisse hängt von Krypto-Expertise und Analysewerkzeugen bei FIU und BaFin ab. Dies sollte ausdrücklich berücksichtigt werden. § 92 betrifft allerdings nur die Aufsichtsbehörden; eine entsprechende ausdrückliche Regelung für die FIU (vgl. Art. 19 Abs. 5 AMLD6) enthält der Entwurf, soweit ersichtlich, nicht.
- **Nationale Risikoanalyse (§ 7 Abs. 2 GwBG-E):** Der Blockchain Bundesverband bringt sich gern mit sektorspezifischer Expertise zu Kryptowerten ein.

Schlussbemerkung

Der Blockchain Bundesverband unterstützt das Ziel, Geldwäsche und Terrorismusfinanzierung wirksam zu bekämpfen. Gerade weil Kryptowerte-Dienstleistungen vollharmonisiert reguliert sind, kommt es jetzt auf klare Begriffe und praxistaugliche Fristen an. Für einen vertieften fachlichen Austausch stehen wir gern zur Verfügung.

Mit freundlichen Grüßen

Blockchain Bundesverband e.V.