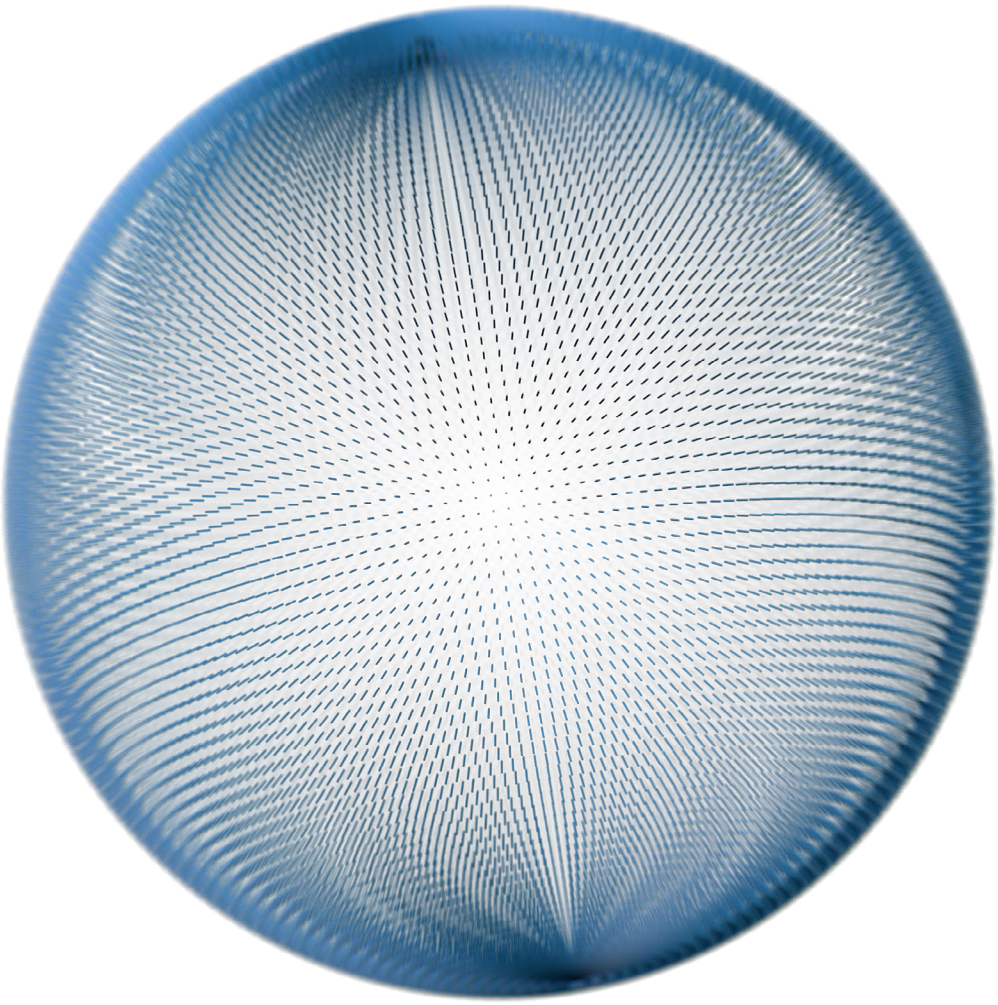
Deloitte.



# Stärkere Regulierung von Krypto-Transaktionen

## Die Neufassung der Geldtransferverordnung (EU) 2015/847

Die geldwäscherechtliche Relevanz von Kryptowerten hat in den letzten Jahren erheblich zugenommen. Die Financial Intelligence Unit („FIU“) erhielt allein im Jahr 2021 rund 5.230[1] Verdachtsmeldungen von Verpflichteten, die als Meldegrund „Auffälligkeiten im Zusammenhang mit Kryptowährungen“ angaben. Nicht nur durch die Umsetzung der 5. Geldwäsche-Richtlinie, sondern auch durch die deutsche Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (KryptoWTransferV[2]) gerieten Kryptowährungen immer weiter in den Fokus der Aufsichtsbehörden. Auf europäischer Ebene empfahl die European Banking Authority (EBA) der Europäischen Kommission bereits Anfang 2019[3], eine Prüfung notwendiger Maßnahmen durchzuführen, um die Risiken im Zusammenhang mit Kryptowerten auf EU-Ebene abzudecken und sich an internationale Standards der Financial Action Task Force (FATF) anzugleichen.

[1] Vgl. FIU, 2021, S. 15.
[2] Vgl. Kryptowertetransferverordnung – KryptoWTransferV vom 24.9.2021, BGBl Nr. 69, S. 4465.
[3] Vgl. EBA, 2019, S. 17 ff.

MAKING AN IMPACT THAT MATTERS since 1845

Damit regulatorische Lücken, wie beispielsweise die unterschiedlichen Zulassungsanforderungen bei der Lizenzvergabe für Dienstleistungen mit Kryptowerten, zwischen den einzelnen Ländern von Kriminellen nicht systemisch ausgenutzt werden können, forderte die Europäische Kommission im Juli 2019[4], eine Reformierung der bestehenden Ermittlungs- und Präventionsverfahren von Geldwäsche und Terrorismusfinanzierung durchzuführen, um somit die Effizienz und Wirksamkeit der Präventionsmaßnahmen zu erhöhen.

Im Jahr 2020 veröffentlichte die Europäische Kommission einen Aktionsplan[5] für einen kohärenten Maßnahmenansatz der EU zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, der auf sechs Säulen aufgebaut ist:

1. Wirksame Umsetzung des bestehenden EU-Rahmens
2. Schaffung eines einheitlichen EU-Regelwerks
3. Einführung einer europäischen Aufsicht
4. Einrichtung eines Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen
5. Durchsetzung strafrechtlicher Bestimmungen und Informationsaustausch auf Unionsebene
6. Stärkung der internationalen Dimension des EU-Rahmens

Um die zweite und die vierte Säule umsetzen zu können, wurde neben anderen Legislativvorschlägen eine Neufassung der Geldtransferverordnung (EU) 2015/847[6] inklusive eines ausgeweiteten Anwendungsbereichs auf Kryptowerte vorgeschlagen. Am 10. Juli 2020 entschloss sich das Europäische Parlament zur Verschärfung der Unionspolitik[7], woraufhin der Rat (Wirtschaft und Finanzen) im November 2020 seine Unterstützung bei der Umsetzung des Aktionsplans mitteilte.[8]


[4] Vgl. Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat COM(2019) 360 final vom 24.7.2019, S. 5; Europäische Kommission: Bericht der Kommission an das Europäische Parlament und den Rat COM(2019) 373 final vom 24.7.2019, S. 26; Europäische Kommission: Bericht der Kommission an das Europäische Parlament und den Rat COM(2019) 371 final vom 24.7.2019, S. 16.
[5] Vgl. Europäische Kommission: Mitteilung der Kommission C(2020) 2800 final vom 7.5.2020, S. 3.
[6] Vgl. Europäische Kommission: Vorschlag zur Verordnung des Europäischen Parlaments und des Rates COM(2021) 422 final vom 20.7.2021.
[7] Vgl. Europäisches Parlament: Resolution on a comprehensive Union policy 2020/2686(RSP), P9_TA(2020)0204 vom 10.7.2020.
[8] Vgl. Rat der Europäischen Union: Schlussfolgerungen des Rates 12608/20 vom 5.11.2020, S. 8.

## Geltungsbereich

Die Kryptowerte unterliegen ähnlichen Risiken in Bezug auf Geldwäsche und Terrorismusfinanzierung und benötigen wie der bisherige elektronische Geldtransfer ebenfalls definierte Anforderungen. Der Vorschlag der Neufassung der Geldtransferverordnung orientiert sich an den aktuellen Standards der FATF zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Krypto-Dienstleister müssen demnach künftig Informationen über Sender (Originator) und Empfänger (Begünstigten) ermitteln, wenn sie Transaktionen abwickeln. Im Fall einer Ermittlung wegen Verdachts auf Geldwäsche oder Terrorismusfinanzierung müssen die Dienstleister die Information auch an die zuständigen Behörden weiterleiten.

Wie in der Empfehlung 16 der FATF („Travel Rule")[9] gefordert, sind Transaktionen mit Kryptowerten stets wie grenzüberschreitende elektronische Geldtransfers zu behandeln – exklusive der Anwendbarkeit vereinfachter Regelungen für innerstaatlichen Geldtransfer.

## Ziele

Mit dem Vorschlag zur Neufassung der Geldtransferverordnung wird der bisherige Anwendungsbereich auf elektronische Geldtransfers nach Art. 4 Nr. 25 der Richtlinie (EU) 2015/2366[10] (Banknoten, Münzen, Giralgeld sowie E-Geld im Sinne von Art. 2 Nr. 2 der Richtlinie 2009/110/EG[11]) um virtuelle Vermögenswerte als Finanzprodukt erweitert. Aktuell erhalten Inhaber von Kryptowerten aufgrund fehlender Rechtsvorschriften noch keinen ausreichenden Schutz vor illegalen Geldströmen. Folglich stellt dies eine Bedrohung des Finanzsektors und des Binnenmarktes dar. Durch die Harmonisierung europäischer Vorschriften im Umgang mit grenzüberschreitenden Transaktionen soll zukünftig ein hohes Maß an Klarheit und Rechtssicherheit für die Krypto-Dienstleister erreicht werden, um insbesondere den Unsicherheiten bei der Vereinbarkeit regulatorischer Vorschriften der einzelnen EU-Staaten, vor allem bei international agierenden Marktteilnehmern, Sorge zu tragen. Die Nachverfolgung der Transfers soll zudem das Risiko der Terrorismusfinanzierung und Geldwäsche deutlich reduzieren. Übergeordnet verfolgt die Europäische Kommission das Ziel, die Integrität und Stabilität des Finanzsystems und das Vertrauen der Marktteilnehmer zu stärken.

## Anforderungen

Die Hauptanforderung der neuen Verordnung betrifft die Nachverfolgbarkeit der Transaktionen für Krypto-Dienstleister, welche bereits seit Jahren für den elektronischen Geldtransfer bestehen.

Anbieter von Krypto-Dienstleistungen (des Originators) haben folgende Informationen vollständig während der Zahlungskette zu übermitteln:

- Name des Originators
- Adresse der elektronischen Geldbörse des Originators bzw. Kontonummer, sofern ein Konto vorhanden ist und für die Abwicklung der Transaktion verwendet wird
- Anschrift des Originators
- Nummer eines amtlichen persönlichen Dokuments des Originators
- Kundennummer oder das Geburtsdatum des Originators
- Geburtsort des Originators
- Name sowie die Kontonummer des Begünstigten, sofern ein Konto vorhanden ist und für die Abwicklung der Transaktion verwendet wird

Anbieter von Krypto-Dienstleistungen (des Begünstigten) haben folgende Verpflichtungen einzuhalten:

- Einrichtung wirksamer Verfahren zur Feststellung der korrekten Angabe der Daten zum Originator in der Zahlungskette inklusive der Nutzung von Dokumenten, Daten oder Informationen aus verlässlichen und unabhängigen Quellen
- Bei Fehlen oder Unvollständigkeit der Daten Sicherstellung der nachträglichen Übermittlung im Anschluss
- Einrichtung einer nachträglichen Überwachung oder einer Echtzeitüberwachung zur Sicherstellung der vorgeschriebenen Angaben zum Originator oder zum Begünstigten

Die Übermittlung der Informationen zum Originator und zum Begünstigten kann in einzelnen Schritten vor oder zeitgleich zur Durchführung der Transaktion erfolgen. Voraussetzung ist, dass diese unverzüglich und gesichert erfolgt. Dies betrifft ebenfalls Sammeltransfers von Kryptowerten.

Falls Angaben zum Originator oder Begünstigten vollständig oder teilweise fehlen, haben Krypto-Dienstleister des Begünstigten und zwischengeschaltete Zahlungsdienstleister risikoorientierte Prozesse bereitzustellen, um den Transfer ausführen, zurückweisen oder aussetzen zu können. Bei fragwürdigen Übermittlungen sind angemessene Maßnahmen durchzuführen, indem beispielsweise verdächtige Transaktionen den zuständigen Behörden unverzüglich gemeldet werden. Bei mehrmaligem Versäumnis der Weiterleitung der vollständigen Angaben sind vom Krypto-Dienstleister des Begünstigten Verwarnungen sowie Fristsetzungen auszusprechen. Weiterhin ist es möglich, den transferierten Kryptowert ohne Bereitstellung an den Begünstigten selbst einzubehalten, bis die zuständige Behörde eine Analyse des Sachverhalts durchgeführt hat.

[9] Vgl. FATF, 2020, S. 78 ff.
[10] Vgl. Richtlinie (EU) 2015/2366 vom 25.11.2015, ABl. S. L 337/35, S. 58.
[11] Vgl. Richtlinie 2009/110/EG vom 16.9.2009, ABl. S. L 267/7, S. 11.

Die Verordnung eröffnet den Mitgliedsstaaten die Option, diese nicht auf den Inlandstransfer von Kryptowerten anzuwenden, wenn folgende Voraussetzungen erfüllt sind:

- Der Krypto-Dienstleister unterliegt der Geldtransferverordnung (EU) 2015/847.
- Der Anbieter von Krypto-Dienstleistungen des Begünstigten kann den Transfer über die Distributed-Ledger-Technologie bis zum Begünstigten eindeutig und individuell zuordnen (Rückverfolgbarkeit).
- Der Kryptotransfer liegt unterhalb des Schwellenwerts von 1.000 EUR.

In diesem Fall sind lediglich die Namen des Originators und des Begünstigten sowie die Kontonummern zu übermitteln. Der Anbieter von Krypto-Dienstleistungen des Originators oder des Begünstigten überprüft die Angaben auf Richtigkeit, wenn

- die erhaltenen Kryptowerte im Tausch gegen Bargeld oder anonymes E-Geld übermittelt werden und
- hinreichende Gründe für einen Verdacht auf Geldwäsche oder Terrorismusfinanzierung bestehen.

Die Europäische Kommission begründet diese Klausel damit, dass die Gefahr für Terrorismusfinanzierung bei kleineren Beträgen geringer ist und daher ein wachsendes Risiko für Krypto-Transfers außerhalb des regulierten Zahlungsverkehrs besteht, wenn zu strenge Identifikationspflichten auferlegt werden. Das Ziel dieses Passus ist es, die Effizienz der Zahlungssysteme zu erhalten und angebotene Dienstleistungen nicht zu beeinträchtigen. Sollten sich allerdings Verdachtsmomente bei diesen Transaktionen ergeben, so findet diese Ausnahme keine Anwendung.

Das Auskunftsersuchen von Behörden des jeweiligen Landes ist unverzüglich zu beantworten. Die Informationen zum Originator und zum Begünstigten des Krypto-Transfers sind zur Ermittlung von Geldwäsche und Terrorismusfinanzierung von den Krypto-Dienstleistern fünf Jahre lang aufzubewahren. Die personenbezogenen Daten sind nach Ablauf der Frist zu löschen, solange dies nicht dem geltenden nationalen Recht entgegensteht. Die Krypto-Dienstleistungen fallen unter die Datenschutz-Grundverordnung (EU) 2016/679[12] sowie die Verordnung (EU) 2018/1725[13] des Europäischen Parlaments und des Rates.

[12] Vgl. Verordnung (EU) 2016/679 vom 27.4.2016, ABl. S. L 119/1.
[13] Vgl. Verordnung (EU) 2018/1725 vom 21.10.2018, ABl. S. L 295/39.

## Herausforderungen in der Praxis

### a) Selfhosted Wallets

Eine der Herausforderungen für die Verpflichteten wird die Anwendung der Inhaberidentifizierung sogenannter „Selfhosted Wallets" sein. Diese werden direkt von Besitzern gehalten, ohne einen Krypto-Dienstleister zu nutzen. Sie gehören nicht zum Verpflichtetenkreis nach den Maßstäben der Europäischen Kommission. Der Vorschlag zur Neufassung der Geldtransferverordnung sieht in seiner jetzigen Fassung keine explizite Ausnahme dieser vor und bietet keinen Praxishinweis für die Verpflichteten im Umgang mit Selfhosted Wallets an. Dies würde zukünftig bedeuten, dass Krypto-Dienstleister eine technische Lösung erstellen müssen, um Urheber- und Empfängerdaten erhalten und verifizieren zu können, bevor ein Transfer von Krypowerten von oder auf eine Selfhosted Wallet vollständig durchgeführt wird. Ob ein Transfer später eingefroren oder weitergeleitet wird, obliegt der institutsspezifischen Risikoeinschätzung des jeweiligen Krypto-Dienstleisters. Hierzu sind entsprechende Sicherungsmaßnahmen zu implementieren, um das Risiko für Geldwäsche, Terrorismusfinanzierung sowie Sanktions- und Embargoumgehung gering zu halten und gleichzeitig größtmögliche Transparenz zu ermöglichen. Die Sicherstellung der Korrektheit personenbezogener Daten wird insofern die Komplexität erhöhen, da sich das Eigentum dieser Wallets durch die Übertragung des Private Key ohne großen Aufwand ändern kann und daher für kriminelle Absichten gut geeignet ist. Die Offenlegungspflichten greifen somit in den Markt ein, da Krypto-Dienstleister mit den Herausforderungen fehlender technischer Mittel (bspw. Vorgaben zu Standards oder Formaten) und zu hoher Kosten bei der Interaktion mit Selfhosted Wallets konfrontiert sind. Eine mögliche Folge wäre, dass Krypto-Dienstleister aufgrund fehlender personenbezogener Daten bei jedem Transfer eine Verdachtsmeldung abgeben müssen oder vorsorglich Überweisungen auf Selfhosted Wallets ganz unterbinden. Es bleibt abzuwarten, ob die Europäische Kommission eine Spezifikation im Umgang mit dieser Problemstellung vornehmen wird.

### b) Personenbezogene Daten

Eine weitere Herausforderung für den Verpflichtetenkreis besteht im Umgang mit den Offenlegungspflichten in Kombination mit dem europäischen Datenschutz gemäß (EU) 2016/679[14] und (EU) 2018/1725[15]. Insbesondere bei international tätigen Unternehmen, die beispielsweise Zweigniederlassungen in Drittstaaten haben, kann dies zu Schwierigkeiten in der Anwendung regulatorischer Vorschriften führen. Sollte eine Transaktion von Kryptowerten ein Verdachtsmoment generieren, so sind die notwendigen Informationen grenzüberschreitend innerhalb der Organisation weiterzuleiten, um den Fall entsprechend bearbeiten zu können und der zuständigen Behörde zu melden. Es ist dabei anzumerken, dass Jurisdiktionen außerhalb der Europäischen Union unterschiedlich robuste Gesetze zum Schutz personenbezogener Daten im nationalen Gesetz verankert haben. Das Unternehmen ist hier verpflichtet, entsprechend der europäischen Datenschutz-Grundverordnung geeignete technische und organisatorische Sicherungsmaßnahmen zu implementieren, um dem Schutz personenbezogener Daten nachzukommen und den Verlust oder die unbefugte Weitergabe zu verhindern.

### c) Kryptografische Protokolle

Die Verarbeitung der Transaktionsdaten inklusive der personenbezogenen Informationen der Endnutzer wird über sogenannte kryptografische Protokolle durchgeführt. Diese kombinieren die Authentifikation von Nutzern und Schlüsselvereinbarungen. Wenn Nutzer Krypowerte über einen Zahlungsdienstleister übertragen wollen, können hierzu unterschiedliche kryptografische Protokolle verwendet werden (bspw. das One-Time-Passwort-Protokoll (OTP), welches für jede Authentifizierung ein anderes Passwort einsetzt). Nicht nur Dienstleister tauschen hiermit untereinander Informationen aus, sondern auch Behörden greifen auf diese zum Zwecke der Strafverfolgung zurück. Neben der Komplexität des Protokolls ist eine weitere Herausforderung für den Verpflichtetenkreis, dass die Europäische Kommission bisher keinen einheitlichen Ansatz für die technische Lösung zur Sammlung von Angaben und deren Austausch spezifiziert hat. Da für jede Protokollart aufgrund ihrer Ausgestaltung ein eigenes Sicherheitsmodell erstellt werden müsste, um die Sicherheitseigenschaften zu identifizieren, ergäbe sich in der Praxis ein hoher Aufwand in der parallelen Anwendung der Varianten für Zahlungsdienstleister und Behörden. Dies hätte ein erhöhtes Risiko von Datenmissbrauch zur Folge, da Kriminelle die fehlende Harmonisierung für sich ausnutzen könnten. Bereits heute besteht im Markt die Problematik, dass verschiedene Protokolle existieren, die nicht miteinander vereinbar sind. Die Spezifikation einer standardisierten Open-Source-Lösung für den Datenaustausch wird von den derzeitigen Marktteilnehmern diskutiert und gefordert.

[14] Vgl. Verordnung (EU) 2016/679 vom 27.4.2016, ABl. S. L 119/1.
[15] Vgl. Verordnung (EU) 2018/1725 vom 21.10.2018, ABl. S. L 295/39.

**d) Finanzieller Aufwand**

Die Ausweitung der Vorschriften zu den bestehenden Informationspflichten auf Kryptotransaktionen und die impliziten Anforderungen bringen aufgrund der Unterschiede in den Merkmalen der Produkte einige Herausforderungen für die verpflichteten Akteure. Eine technische sowie organisatorische Implementierung der Travel Rule erzeugt einen hohen Aufwand und entsprechende Kosten. Da beides gegebenenfalls nur von größeren Marktteilnehmern geleistet werden kann und folglich andere Dienstleister vom Markt ausschließt, könnte dies zu einer Marktbeeinflussung führen. Die Europäische Kommission geht derzeit bei der Vereinheitlichung europäischer Rechtsvorschriften von einer kurzzeitigen Kostenerhöhung für die Verpflichteten bei grenzüberschreitenden Dienstleistungen aus.[16] Das Ziel des präventiven Ansatzes der neuen Verordnung soll auch sein, dass keine zusätzliche Belastung für die Zahlungsdienstleister auftritt und die Regulatorik in einer angemessenen Verhältnismäßigkeit steht.[17] Ob die notwendigen Kosten zur Implementierung der Travel Rule aufgrund von Erfahrungswerten in der mittelfristigen Planung gesenkt werden können, bleibt abzuwarten.

**Fazit**

Die Europäische Kommission hat mit ihrem Vorschlag für die Erweiterung der Geldtransferverordnung die gemeinsamen Risiken des Geld- und Kryptotransfers erkannt und die Empfehlung 16 der FATF[18] vollständig übernommen. Um bei der Übertragung von Kryptowerten eine Nachverfolgbarkeit der Daten zu garantieren, sind Krypto-Dienstleister nun verpflichtet, die erforderlichen Sorgfaltsanforderungen gegenüber ihren Kunden in Bezug auf das „Know Your Customer (KYC)"-Prinzip anzuwenden, um der Bekämpfung von Geldwäsche und Terrorismusfinanzierung gerecht zu werden. Für Deutschland wird die Verordnung, im Gegensatz zu anderen EU-Staaten, voraussichtlich für weniger Überraschung sorgen, da bereits am 1. Oktober 2021 die KryptoWTransferV in Kraft getreten ist, die die Travel Rule der FATF bereits umgesetzt hat. Schon bei der Einführung der KryptoWTransferV zeigte sich, dass die traditionellen IT-Lösungen in der Compliance die komplexen Strukturen der Blockchain und Beziehungen der Marktteilnehmer untereinander nicht abbilden können. Auch die Frage zum Echtzeitmonitoring wurde in diesem Kontext häufig diskutiert. Neben diesen Herausforderungen werden zukünftig auch andere rechtliche Unsicherheiten wie der Umgang mit Selfhosted Wallets, der Datenschutz-Grundverordnung bei grenzüberschreitenden Transaktionen und auch die Spezifikation einer standardisierten Open-Source-Lösung zur Datenverarbeitung bestehen.

Laut Länderbericht der FATF über die Geldwäscheprävention in Deutschland („Mutual Evaluation Report")[19] von August 2022 sind die Mitgliedsstaaten innerhalb der EU die wichtigsten Kooperationspartner für Deutschland, um internationale Kriminalität zu identifizieren. Mit einer einheitlichen Umsetzung der Travel Rule in das nationale Gesetz aller Mitgliedsstaaten kann damit die europäische Zusammenarbeit der Ermittlungsbehörden gestärkt werden, um verdächtige Transaktionen und Gruppierungen rechtzeitig zu entdecken und strafrechtlich zu verfolgen. Inwieweit durch die Harmonisierung der europäischen Vorschriften im Umgang mit grenzüberschreitenden Krypto-Transaktionen das übergeordnete Ziel der Integrität und Stabilität des Finanzsystems erreicht werden kann, wird sich spätestens in der praktischen Umsetzung der Verordnung zeigen.

Ergänzt wird das Regulierungspaket durch das DLT-Pilotregime[20], das den Aufbau von Finanzmarktinfrastrukturen auf Basis der Distributed-Ledger-Technologie (DLT) regelt. Die Neufassung der Geldtransferverordnung soll zusammen mit der Verordnung über Märkte für Krypto-Assets (MiCA) veröffentlicht und voraussichtlich Mitte 2024 in nationales Recht übernommen werden. In Zusammenspiel der beiden Verordnungen werden übergeordnet bessere Rechtsklarheit und -sicherheit geschaffen und die Überwachungstätigkeiten der einzelnen Aufsichtsbehörden gestärkt. Ob die noch offenen Fragen, wie z.B. die Behandlung von Selfhosted Wallets und Kryptowerten, die außerhalb der derzeitigen Definition gemäß MiCA[21] fallen (z.B. Stable Coins), bis dahin geklärt sind, bleibt abzuwarten.

[16] Vgl. Europäische Kommission: Vorschlag zur Verordnung des Europäischen Parlaments und des Rates COM(2021) 422 final vom 20.7.2021, S. 3.
[17] Vgl. Europäische Kommission: Vorschlag zur Verordnung des Europäischen Parlaments und des Rates COM(2021) 422 final vom 20.7.2021, S. 16.
[18] Vgl. FATF, 2020, S. 79 ff.
[19] Vgl. FATF, 2022, S. 214.
[20] Vgl. Europäische Kommission, Vorschlag zur Verordnung des Europäischen Parlaments und des Rates COM(2020) 593 final vom 24.9.2020, S. 40 ff.
[21] Vgl. Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates COM(2020) 594 final vom 24.9.2020.

## Literaturverzeichnis


### Rechtsquellen

- Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG vom 16.9.2009 (ABl. S. L 267/7).
- Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006 vom 20.5.2015 (ABl. S. L 141/1).
- Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG vom 25.11.2015 (ABl. S. L 337/35).
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) vom 27.4.2016 (ABl. S. L 119/1).
- Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG vom 23.10.2018 (ABl. S. L 295/39).
- Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich (Geldwäschegesetzmeldepflichtverordnung-Immobilien – GwGMeldV-Immobilien) vom 31.8.2020 (BGBl I Nr. 40 S. 1965).
- Vorschlag zur Verordnung des Europäischen Parlaments und des Rates on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 vom 24.9.2020 (COM(2020) 593 final).
- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Pilotregelung für auf der Distributed-Ledger-Technologie basierende Marktinfrastrukturen vom 24.9.2020 (COM(2020) 594 final).
- Vorschlag zur Verordnung des Europäischen Parlaments und des Rates zur Errichtung der Behörde zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 vom 20.7.2021 (COM(2021) 421 final).
- Vorschlag zur Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte (Neufassung) vom 20.7.2021 (COM(2021) 422 final).
- Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung – KryptoWTransferV) vom 24.9.2021 (BGBl Nr. 69 S. 4465).

### Verlautbarungen

- EBA (2019): Report with advice for European Commission on crypto assets.
- Mitteilung der Kommission an das Europäische Parlament und den Rat über Wege zu einer besseren Umsetzung des Rechtsrahmens der EU für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung vom 24.7.2019 (COM(2019) 360 final).
- Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung aktueller Fälle von mutmaßlicher Geldwäsche unter Beteiligung von Kreditinstituten aus der EU vom 24.7.2019 (COM(2019) 373 final).
- Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung des Rahmens für die Zusammenarbeit zwischen den zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU) vom 24.7.2019 (COM(2019) 371 final).
- Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector vom 4.10.2019 (JC2019 59).
- Mitteilung der Kommission zu einem Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung vom 7.5.2020 (C(2020) 2800 final).
- Resolution on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments vom 10.7.2020 (2020/2686(RSP)), P9_TA(2020)0204.
- Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – EU-Strategie für eine Sicherheitsunion vom 24.7.2020 (COM(2020) 605 final).
- FATF (2020): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations.
- Schlussfolgerungen des Rates zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung vom 5.11.2020 (12608/20).
- FIU (2021): Jahresbericht 2021.
- FATF (2022): Mutual Evaluation Report Germany.

### Internetquellen

- Digitales Finanzwesen: Einigung über die europäische Verordnung über Kryptowerte (MiCA) – Rat der EU, abgerufen unter: https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/ (23.12.2022).
- Commission launches first Academy for digital finance supervisory – Europäische Kommission, abgerufen unter: https://commission.europa.eu/news/commission-launches-first-academy-digital-finance-supervisory-authorities-2022-10-24_en (23.12.2022).

# Ihre Ansprechpartner

**Dr. Christoph Wronka**
Director | Financial Advisory | Forensic FSI | Lead Blockchain, Digital Assets & Financial Crime
Tel: +49 151 58075428
cwronka@deloitte.de

**Florian Naas**
Director | Risk Advisory | Financial Crime | Regulatory & Legal Support
Tel: +49 151 58075478
flonaas@deloitte.de

**Anna-Lena Wiegand**
Senior Consultant | Financial Advisory | Forensic FSI | Blockchain, Digital Assets & Financial Crime
Tel: +49 151 19176393
anwiegand@deloitte.de

**Lena Mann**
Senior Consultant |Risk Advisory | Financial Crime | Regulatory & Legal Support
Tel: +49 151 14880885
lmann@deloitte.de

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL"), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation"). DTTL (auch „Deloitte Global" genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeiterinnen und Mitarbeiter liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte das Leitbild „making an impact that matters" täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL"), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation") erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 03/2023