



MASTER THESIS | MASTER'S THESIS

Titel | Title

Überprüfung der Betroffenenrechte gemäß EU-Datenschutz-Grundverordnung in der Deutschen Kryptowertetransferverordnung sowie insbesondere in der MiCA-Verordnung

verfasst von | submitted by

Mag.iur. Eliza Irene Loeschnigg

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 992 942

Universitätslehrgang lt. Studienblatt | Post-
graduate programme as it appears on the stu-
dent record sheet:

Informations- und Medienrecht

Betreut von | Supervisor:

Prof. Dr. Thomas Hoeren

MASTER THESIS

Titel der Master Thesis

Überprüfung der Betroffenenrechte
gemäß EU-Datenschutz-Grundverordnung
in der Deutschen Kryptowertetransferverordnung sowie
insbesondere in der MiCA-Verordnung

verfasst von
Eliza Irene Löschnigg

angestrebter akademischer Grad
Master of Laws (LL.M.)

Wien, 2024

Studienkennzahl lt. Studienblatt: UA 992 942

Universitätslehrgang lt. Studienblatt: Informations- und Medienrecht

Betreut von: Prof. Dr. Thomas Hoe

Inhaltsverzeichnis

1. EINLEITUNG	3
2. EINFÜHRUNG	4
3. VERORDNUNG ÜBER VERSTÄRKTE SORGFALTSPFLICHTEN BEI DEM TRANSFER VON KRYPTOWERTEN (KRYPTOWERTETRANSFERVERORDNUNG – KRYPTOWTRANSFERV)	7
3.1. ZUSAMMENFASSUNG DER KRYPTOWERTETRANSFERVERORDNUNG DEUTSCHLAND.....	7
3.2. BEGRÜNDUNG FÜR DEN ER Lass DER KRYPTOWERTETRANSFERVERORDNUNG.....	10
3.3. STELLUNGNAHME ZUM REFERENTENTWURF DER KRYPTOWERTETRANSFERVERORDNUNG	11
4. VERORDNUNG ÜBER MÄRKTE FÜR KRYPTOWERTE – (MICA)	15
4.1. ZUSAMMENFASSUNG DER MiCA-VERORDNUNG.....	15
4.1.1 Pflichten für Emittenten von Krypto-Werten.....	17
4.1.2. Pflichten von Krypto-Dienstleistern	18
4.1.3 Rechte von Verbrauchern.....	19
4.1.4. Überwachung und Durchsetzung	20
4.2. BEGRÜNDUNG FÜR DEN ER Lass DER MiCA-VERORDNUNG.....	21
5. DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)	23
5.1. ALLGEMEINES ZUR DSGVO	23
5.2. ZUSAMMENFASSUNG DER BETROFFENENRECHTE IN DER DSGVO	24
6. TRANSPARENZ VERSUS SCHUTZ VON DATEN	28
6.1. ANALYSE DER VEREINBARKEIT DSGVO UND KRYPTOWTRANSFERV	28
6.2. ANALYSE DER VEREINBARKEIT DSGVO UND MiCA-VO	31
6.3. EXKURS - EUGH URTEIL ZUR UNVEREINBARKEIT DER EU-GELDWÄSCHERICHTLINIE MIT DER GRC	35
7. CONCLUSIO	37
8. LITERATURVERZEICHNIS	40

1. Einleitung

Die Kryptowertetransferverordnung als auch die MiCA-Verordnung betreffen einen bis dato noch nicht ausreichend regulierten Bereich. Da Kryptowerte im Allgemeinen nicht über Bankinstitute gehandelt werden, mangelt es an ausreichenden Maßnahmen, die dem Schutz vor Geldwäsche und Terrorismusfinanzierung dienen. Diese Lücke zu schließen und den Transfer von Kryptowährungen gesetzlich überwachen zu können, ist das Ziel der Kryptowertetransferverordnung sowie auch der MiCA-Verordnung. Durch die EU-Datenschutz-Grundverordnung wiederum werden die Rechte von Betroffenen festgelegt. Sie reguliert den Umgang mit personenbezogenen Daten.

Die vorliegende Arbeit befasst sich mit der Frage, inwiefern sich die Bestimmungen gemäß der Kryptowertetransferverordnung in Deutschland in Bezug auf die Betroffenenrechte gemäß der EU-Datenschutz-Grundverordnung sowie der MiCA-Verordnung vereinbaren lassen bzw. im Widerspruch zu diesen stehen und inwiefern die Kryptowertetransferverordnung als auch die MiCA-Verordnung unter diesem Gesichtspunkt geeignet sind, dem Risiko von Geldwäsche und Terrorismusfinanzierung zu begegnen, ohne dabei Betroffenenrechte zu verletzen. Es wird erörtert, inwiefern die Forderung nach Transparenz dem Schutz personenbezogener Daten entgegensteht. Im Zuge der Analyse wird eine allfällig bestehende Diskrepanz zwischen der Überwachung des Handels von Kryptowerten und dem Schutz des Einzelnen herausgearbeitet.

Bevor für die Überprüfung der Betroffenenrechte gemäß der EU-Datenschutz-Grundverordnung in der Kryptowertetransferverordnung als auch in der MiCA-Verordnung alle drei Verordnungen zusammengefasst werden, sollen zunächst einführende Worte zu Kryptowerten einen groben Überblick über die verschiedenen Formen von Kryptowerten und deren Verwendungszwecke schaffen.

Als Exkurs wird ein Urteil des Europäischen Gerichtshofes zusammengefasst, welches sich mit der Unvereinbarkeit der EU-Geldwäscherichtlinie sowie der GRC auseinandersetzt. Schließlich wird in der Conclusio das Ergebnis der Forschungsarbeit zusammengefasst sowie die persönliche Meinung des Autors erläutert.

2. Einführung

Sowohl taucht der Begriff „Kryptowerte“ in privaten Gesprächen wie im öffentlichen Diskurs immer häufiger auf, als auch erfreut sich der Handel mit Kryptowerten wachsender Bedeutung. Chancen und Risiken der digitalen Vermögenswerte werden reflektiert und auf unterschiedlichen Plattformen besprochen. Als bekanntestes Beispiel von Kryptowerten lassen sich wohl Kryptowährungen nennen. Die Möglichkeiten der Verwendung von Kryptowerten können jedoch als vielfältig angesehen werden. Je nach Verwendungszweck lassen sich Kryptowerte in unterschiedliche Kategorien einteilen. Dieses Kapitel soll einen Überblick über diese Zuordnung, wie von Khayat beschrieben, bieten.¹

Eine Form von Kryptowerten sind die oben genannten Kryptowährungen, auf Englisch Currency-Token genannt. In dieser Kategorie stellt wiederum der Bitcoin wohl die bekannteste Art von Kryptowährungen dar. Weitere Beispiele sind Ether, Litecoin oder Dogecoin. Ein Ziel des Erwerbs von Kryptowährungen kann der Wertaufbewahrung dienen. Allerdings bestimmt sich der Wert durch Angebot und Nachfrage, wodurch mit starken Schwankungen zu rechnen ist.

Um diesen Schwankungen zu begegnen, hat sich eine Form von Currency-Token etabliert, die sich aufgrund der Koppelung an einen anderen Wert (insbesondere an eine amtliche Währung), zum Beispiel an den US-Dollar, sohin durch eine verlässlichere Stabilität auszeichnet.² Solche Kryptowerte werden auch „Stablecoins“ oder E-Geld-Token genannt. Beispiele für (bereits mit der MiCA-VO im Einklang stehende) Stablecoins sind Monerium und EURC.

Aufgrund der schwankenden Werte eignen sich (übliche) Kryptowährungen besonders für Spekulationen. Neben dem Zweck der Wertaufbewahrung, wird mit dem Handel von Kryptowährungen häufig das Ziel verfolgt, Gewinne zu lukrieren und sie als Wertanlage zu nutzen, da die Chance der Wertsteigerung besteht.³

Eine dritte Möglichkeit des Einsatzes von Kryptowährungen besteht in der Bezahlungsfunktion, wobei hier wiederum die Wertschwankungen die Eignung als

¹Vgl. Khayat 2023, 15ff

²Vgl. Khayat 2023, 19f

³Vgl. Khayat 2023, 19

Geldersatz einschränken.⁴ Dennoch sind Kryptowährungen, obwohl als Alternative zu staatlich kontrollierten Währungen eingesetzt, in einigen Ländern wie El Salvador oder Panama mittlerweile als gesetzliches Zahlungsmittel anerkannt. In Deutschland ist das zwar nicht der Fall, aber eine Verwendbarkeit in einem gewissen eingeschränkten Rahmen ist sehr wohl möglich und geltende rechtliche Regelungen können angewendet werden. Wird etwa eine Bezahlung in Kryptowährungen als Gegenleistung getätigt, handelt es sich rechtlich um einen Tausch, werden Kryptowährungen erstanden, kann dieser Erwerb rechtlich analog zu einem Rechtskauf behandelt werden.⁵

Aufgrund der Dezentralisierung sowie der äußerst schwierigen Nachverfolgbarkeit von Transaktionen bestimmter Kryptowährungen anhand unter anderem deren besonders gesicherter Blockchain-Technologie, wie zum Beispiel der Krypto-Währung „Monero“, wird diese auch besonders häufig im rechtsfreien Raum zum Erwerb illegaler Güter verwendet. In diesen Fällen ist die Anwendung geltender rechtlicher Regelungen (noch) nicht möglich.

Technologisch betrachtet, werden Kryptowährungen dezentral auf der Blockchain gespeichert. Eine Blockchain ist eine Datenbank, eine Liste von in Blöcken gespeicherten Datensätzen⁶, die als öffentliches Kontenbuch dezentral geführt wird⁷, und stellt die am häufigsten genutzte Basis für den Handel mit Kryptowerten dar⁸.

Als Security-Token, Equity-Token oder Investment-Token werden jene Kryptowerte bezeichnet, die sich aufgrund ihres Verwendungszwecks in eine zweite Kategorie einordnen lassen. Personen erwerben mit dem Kauf mitgliedschaftliche und/oder vermögensrechtliche Ansprüche. Die Funktion dieser Art von Kryptowerten ähnelt somit der von Wertpapieren wie Aktien und Anleihen.⁹

Als dritte Kategorie können Utility-Token bzw. Nutzungstoken oder digitale Gutscheine genannt werden. Bei dieser Form geht es darum, sich einen Zugang zu Produkten

⁴Vgl. Khayat 2023, 19

⁵Vgl. Khayat 2023, 9ff

⁶Vgl. Khayat 2023, 10

⁷Vgl. Khayat 2023, 17

⁸Vgl. Khayat 2023, 18

⁹Vgl. Khayat 2023, 20

oder Dienstleistungen eines Unternehmens zu sichern (unabhängig davon, ob diese bereits existieren oder zukünftig angeboten werden). Diese Kryptowerte können auch als Zahlungsmittel eingesetzt werden, jedoch nur auf bestimmten Plattformen (z.B. als In-Game-Währungen). Da der Wert der Utility-Token auch schwanken kann, ist eine Nutzung als Investment prinzipiell möglich, nicht aber primäre Funktion.¹⁰

In einer vierten Kategorie werden sogenannte hybride Formen von Token subsumiert, die eine Mischform darstellen, also mehrere Funktionen erfüllen können, und sich somit der Zuordnung in eine der oben beschriebenen Gruppen entziehen. Darüber hinaus entwickeln sich weitere neue Typen, wie Non-Fungible Token (NFTs), welche dazu geeignet sind, durch digitale Speicherung unter Einsatz der Blockchain-Technologie, eine Inhaber*innenschaft an einem Kunstwerk festzulegen.¹¹

Als Akteur*innen bei Transfers von Kryptowerten lassen sich Emittent*innen, Dienstleister und Nutzer*innen nennen. Erstere sind Personen oder Institute, welche die Token „schaffen“, in der Blockchain hinterlegen und ausgeben. Kryptowertedienstleister betreiben als Unternehmen Bankgeschäfte mit Kryptowerten. Sie speichern die für den Handel nötigen öffentlichen und privaten kryptografischen Schlüssel. Öffentliche Schlüssel oder Public Keys können in ihrer Funktionsweise mit Kontonummern, privaten Schlüsseln oder Private Keys mit Pin-Codes verglichen werden. Des Weiteren können Dienstleister den Transfer (mehrmaliges Weitersenden) von Token zwischen unternehmenseigenen Public Keys anbieten (sodass am Ende die/der Nutzer*in gleichwertige Token erhält, die Transaktionshistorie jedoch verfälscht wird) oder lediglich die Software und Hardware bereitstellen.¹² Nutzer*innen können mit dem Handel von Kryptowerten unterschiedliche Ziele verfolgen, gleichzeitig kann davon ausgegangen werden, dass Nutzer*innen jedenfalls *„[...] als Anleger mit einem Interesse an Wertsteigerung aktiv [sind], auch wenn dies teilweise nicht dem eigentlichen Zweck der Token entspricht.“*¹³

¹⁰Vgl. Khayat 2023, 21

¹¹Vgl. Khayat 2023, 22f

¹²Vgl. Khayat 2023, 23ff

¹³Vgl. Khayat 2023, 25

3. Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung – KryptoWTransferV)

3.1. Zusammenfassung der Kryptowertetransferverordnung Deutschland

Kryptowerte haben in den letzten Jahren für den Finanzmarkt an Bedeutung gewonnen. Khayat begründet die zunehmende Relevanz mit dem Aufkommen des Bitcoins 2008.¹⁴

Kryptowerte eröffnen neue Chancen, bieten großes Potenzial und zeichnen sich durch zahlreiche Einsatzmöglichkeiten aus. Gleichzeitig ist ihnen jedoch ein gewisses Risiko immanent: einerseits bestehen Unsicherheiten für Anleger*innen und andererseits birgt die Anonymität im Handel mit Kryptowerten die Gefahren kriminellen Missbrauchs.¹⁵ Es ist zu befürchten, dass weitgehende Anonymität der Beteiligten und fehlende Möglichkeit Rückschlüsse auf die Identität von Nutzer*innen ziehen zu können, für organisierte Kriminalität besonders attraktiv erscheint und Kryptowerte für Geldwäsche und Terrorismusfinanzierung eingesetzt werden.¹⁶

Als Reaktion auf diesen Umstand werden gesetzliche Regelungen auf nationaler als auch auf europäischer Ebene diskutiert und beschlossen.¹⁷ Regulierungsinitiativen zielen darauf ab, dass Kryptowertetransfers stets rückverfolgbar sein sollen. Für diesen Zweck ist es nötig, dass personenbezogene Daten erhoben und verarbeitet werden.¹⁸ Maßnahmen sowohl hinsichtlich des Schutzes für Anleger*innen als auch hinsichtlich der Aufdeckung bzw. Abwendung krimineller Handlungen wurden gesetzt.¹⁹

Das deutsche Bundesministerium für Finanzen erachtete es als notwendig, den Bereich der Transaktionen mit Kryptowerten zu regulieren, mit eben dieser Begründung: um kriminelle Aktivitäten zu entdecken und die Gefahr einer missbräuchlichen Anwendung möglichst unterbinden zu können.²⁰

¹⁴Vgl. Khayat 2023, 97

¹⁵Vgl. Khayat 2023, 37

¹⁶Vgl. Khayat 2023, 36 und 61

¹⁷Vgl. Khayat 2023, 97

¹⁸Vgl. Khayat 2023, 61

¹⁹Vgl. Khayat 2023, 97

²⁰Vgl. Khayat 2023, 61

Die am 1. Oktober 2021 in Deutschland in Kraft getretene Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung - KryptoWTransferV), im Folgenden KryptoWTransferV genannt, hat dementsprechend explizit das Ziel, Geldwäsche und Terrorismusfinanzierung zu verhindern. Um dem, aufgrund der Anonymität der Beteiligten eines Kryptowertetransfers, als erhöht einzuschätzenden Risiko Rechnung zu tragen, wird durch die Verordnung die Bekanntgabe gewisser Informationen analog zur deutschen Geldtransferverordnung, im Folgenden GTVO genannt, angeordnet. So legt die KryptoWTransferV fest, dass bestimmte Daten der an der Transaktion Beteiligten, gegenseitig übermittelt werden müssen und rückverfolgbar sein müssen.²¹ Konkret bedeutet das, „[...] dass Kryptowertedienstleister, die im Auftrag eines Auftragsnehmers Kryptowerte übertragen, dem Kryptowertedienstleister, der auf Seiten des Empfängers handelt, Angaben zum Namen, zur Anschrift und zur Kontonummer (z.B. den öffentlichen Schlüssel) des Auftraggebers und zum Namen und zur Kontonummer (z.B. öffentlicher Schlüssel) des Begünstigten zeitgleich und sicher übermitteln müssen. Der Kryptowertedienstleister, der für den Begünstigten handelt, hat sicherzustellen, dass er die Informationen zu Auftraggeber und Begünstigten auch erhält und speichert.“²²

Beide Seiten – sowohl Auftraggeber*innen als auch Begünstigte – sind verpflichtet bestimmte personenbezogene Daten zu erheben, andernfalls darf ein Transfer nicht durchgeführt werden bzw. muss gestoppt werden.²³

Durch die Einhaltung dieser erhöhten Sorgfaltspflichten soll sichergestellt werden, dass keine illegalen Handlungen mittels Kryptowerten finanziert werden. Zu diesem Zweck wird durch die KryptoWTransferV festgelegt, dass die oben genannte Informationen über Auftraggeber*in und Empfänger*in erhoben, gespeichert und übermittelt werden müssen, um Transparenz und Rückverfolgbarkeit zu gewährleisten.

Unter § 3 der KryptoWTransferV werden die Pflichten festgelegt, die bei einer Transaktion zwischen zwei Kryptowertedienstleistern zu erfüllen sind, wobei unter § 2

²¹Vgl. Bundesministerium der Finanzen 2021a

²²Vgl. Bundesministerium der Finanzen 2021a

²³Vgl. Khayat 2023, 61f

leg.cit. eine Begriffsbestimmung vorgenommen wird. Unter § 4 leg.cit. finden sich die erhöhten Sorgfaltspflichten von Auftraggeber*innen und Begünstigten im Falle, dass zumindest auf einer Seite kein Unternehmen involviert ist.²⁴

Unter § 3 der KryptoWTransferV wird auf die Artikel 4 und 6 bis 9 der GTVO verwiesen.²⁵ Demnach gelten für „Verpflichtete“ bei Kryptowertetransfers dieselben Pflichten wie in der GTVO beschrieben. „Verpflichtete“ werden gemäß § 2 Absatz 1 Nummer 1 und 2 des Geldwäschegesetzes bestimmt²⁶ und als Kredit- oder Finanzdienstleistungsinstitute nach dem Kreditwesengesetz definiert²⁷.

Die Pflichten für Zahlungsdienstleister der Auftraggeber*innen gemäß § 3 KryptoWTransferV und wie in Artikel 4 (Nennung der Pflichten) und 6 (Geldtransfers nach außerhalb der Union) der GTVO beschrieben, gelten demnach ebenso für Zahlungsdienstleister, die im Rahmen von Kryptowertetransfers für die Auftraggeber*innen tätig sind. So ist vorgeschrieben, dass Zahlungsdienstleister der Auftraggeber*innen bestimmte Daten zu Auftraggeber*innen (Name, Kontonummer oder Transaktionskennziffer, Anschrift, Dokumentennummer, Kund*innennummer oder Geburtsdatum und -ort) und zu Begünstigten (Name und Kontonummer oder Transaktionskennziffer) übermitteln und auf deren Richtigkeit überprüfen müssen. Andernfalls dürfen Transfers nicht durchgeführt werden.²⁸

Für Zahlungsdienstleister, die im Auftrag von Begünstigten in den Transfer von Kryptowerten involviert sind, gelten die Vorschriften der Artikel 7, 8 und 9 der GTVO. So muss der Zahlungsdienstleister feststellen, ob die vorgeschriebenen Angaben zu Auftraggeber*innen und Begünstigten vollständig gemacht wurden und hat unter gewissen Bedingungen die Richtigkeit der Daten zu überprüfen. Weiters ist in Artikel 8 und 9 geregelt, wie bei fehlenden Daten vorgegangen werden muss (risikoorientierte Vorgehensweise und Abschätzung durch den Dienstleister der/des Begünstigten).²⁹

²⁴s. BGBl. Nr.69/2021

²⁵s. BGBl. Nr.69/2021

²⁶s. BGBl. Nr.69/2021

²⁷Vgl. Geldwäschegesetz – GwG

²⁸Vgl. Verordnung (EU) 2015/847

²⁹Vgl. Verordnung (EU) 2015/847

3.2. Begründung für den Erlass der Kryptowertetransferverordnung

Wie bereits erwähnt, liegt der Grund für den Erlass der KryptoWTransferV darin, eine rechtssichere Regulierung des Kryptowährungsmarktes in Deutschland zu schaffen. Der Handel mit Kryptowerten eröffnet die Möglichkeit zu Innovationen, birgt aber auch Risiken, insbesondere das Themenfeld Einsatz von Kryptowerten für kriminelle Zwecke (Geldwäsche und Terrorismusfinanzierung), aber auch den Bereich des Verbraucher*innenschutzes betreffend. Als besonderer Risikofaktor wird die Anonymität der Transaktionsbeteiligten gesehen (ein Umstand, der bei Geldtransfers nicht besteht).³⁰

Das Bundesministerium für Finanzen in Deutschland begründet also den Erlass der KryptoWTransferV mit der gestiegenen Bedeutung von Kryptowerten für den Finanzmarkt und dem Fehlen von Regelungen im Gegensatz zu Geldtransfers (eine Lücke, die trotz EU-Geldwäscherichtlinie und GTVO bestehe), sowie den besonderen Risiken bezüglich eines kriminellen Einsatzes von Kryptowerten aufgrund – der im Wesen des Kryptowertetransfers inne liegenden Möglichkeiten - der Anonymität und der raschen weltweiten Abwicklung über virtuelle Plattformen.³¹

In der Begründung des Bundesministeriums wird auf den Unterschied zwischen anonym und pseudonym hingewiesen, wobei bei der Verwendung eines Pseudonyms eine Analyse von Transaktionsmustern in öffentlichen Blockchains und eine gewisse Rückverfolgbarkeit grundsätzlich möglich sei.³²

Aus den angeführten Gründen sieht das Bundesministerium die Verordnung als alternativlos und verhältnismäßig. Es werden Pflichten für die in einen Kryptowertetransfer involvierten Personen und Unternehmen zur Erhebung, Speicherung und Übermittlung von Daten festgelegt. Unterschieden wird, ob ein Transfer zwischen Kryptowertedienstleistern stattfindet oder ein Transfer getätigt wird, an dem nicht ausschließlich Finanzdienstleister beteiligt sind. Bei letzterem haben Verpflichtete, deren Gegenüber ohne Kryptowertedienstleister handeln, eine Risikobewertung vorzunehmen und entsprechende Maßnahmen zu setzen.³³

³⁰Vgl. Bundesministerium der Finanzen 2021b

³¹Vgl. Bundesministerium der Finanzen 2021b

³²Vgl. Bundesministerium der Finanzen 2021b

³³Vgl. Bundesministerium der Finanzen 2021b

3.3. Stellungnahme zum Referentenentwurf der Kryptowertetransferverordnung

Die Stellungnahmen zum Referentenentwurf, die vor dem finalen Erlass der KryptoWTransferV veröffentlicht werden, fielen tendenziell skeptisch aus.

Grundsätzlich richtet sich die Kritik weniger gegen eine Regulierung, die zum Teil, wie etwa von der Deutschen Börse Group sogar ausdrücklich begrüßt und als Maßnahme zur Steigerung des Vertrauens in Kryptowerte eingeschätzt wird. Das Ziel der Verhinderung krimineller Handlungen durch Rückverfolgbarkeit der Transfers wird als positiv hervorgehoben.³⁴ Ebenso wird ein risikobasierter Ansatz unterstützt, sowie die Anlehnung an Geldwäschegesetz und GTVO, jedoch hinterfragt, inwiefern von einer Analogie auszugehen gerechtfertigt ist. So ist der Verband der Auslandsbanken in Deutschland e.V. der Meinung, dass die KryptoWTransferV durch das Fehlen von Ausnahmen von der Überprüfungspflicht eben nicht dem risikobasierten Grundgedanken der GTVO entspricht.³⁵ Die Deutsche Kreditwirtschaft bezweifelt, ob die Anwendung der GTVO bei Kryptowertetransfers sachgerecht wäre.³⁶

Weiters werden folgende Aspekte in den Stellungnahmen thematisiert: Die Frage nach der technischen Umsetzbarkeit wird gestellt, ein Wettbewerbsnachteil für deutsche Unternehmer*innen und die Ablehnung nationaler statt internationaler Regulierung festgestellt, die Gefahr einer Abwanderung von Marktteilnehmer*innen in intransparente Infrastrukturen befürchtet, das tatsächliche Missbrauchsrisiko durch Kryptowerte hinterfragt und die datenschutzrechtliche Perspektive angesprochen.

In den Stellungnahmen vom Verein Bitkom³⁷, der Bundesverband der Geldwäschebeauftragten³⁸, der Deutschen Kreditwirtschaft³⁹, Kapilendo⁴⁰, sowie Lindemann, Schwernnicke & Partner⁴¹ wird das Fehlen der technischen Voraussetzungen konstatiert. Die vorgeschriebene Datenübermittlung könne aufgrund der dezentralen Abwicklungsinfrastruktur nicht durchgeführt werden, geeignete technische Standards und ein gemeinschaftlich verwaltetes Übermittlungssystem

³⁴Vgl. Deutsche Börse Group 2021

³⁵Vgl. Verband der Auslandsbanken in Deutschland e.V. 2021

³⁶Vgl. Die Deutsche Kreditwirtschaft 2021

³⁷Vgl. Bitkom Bundesverband 2021

³⁸Vgl. Bundesverband der Geldwäschebeauftragten e.V. 2021

³⁹Vgl. Die Deutsche Kreditwirtschaft 2021

⁴⁰Vgl. Kapilendo AG 2021

⁴¹Vgl. LSP 2021

seien Voraussetzung, aber nicht vorhanden.

Bezüglich der Überlegungen möglicher Auswirkungen der KryptoWTransferV auf den Wirtschaftsstandort Deutschland sind sich Bitkom⁴², Blockchain Bundesverband e.V.⁴³, Deutsche Kreditwirtschaft⁴⁴, Kapilendo⁴⁵, Verband der Auslandsbanken in Deutschland e.V.⁴⁶ und der Wirtschaftsrat der CDU e.V.⁴⁷ einig, dass die Verordnung einen signifikanten Wettbewerbsnachteil für deutsche Verpflichtete mit sich bringen würde. Eine internationale, statt einer nationalen Lösung wird als erstrebenswert erachtet. Die kommentierenden Institute plädieren zum Zeitpunkt des damaligen Erlasses der KryptoWTransferV für eine idealerweise weltweit, zumindest aber EU-weit einheitliche Lösung. Dieser Auffassung entgegnet Khayat, dass das hohe Missbrauchsrisiko das zeitnahe Aktivwerden des Bundesministeriums rechtfertigt und ein Abwarten einer europaweiten Einigung ablehnt.⁴⁸

Der Bundesverband der Geldwäschebeauftragten⁴⁹ und Kapilendo⁵⁰ warnen vor der Gefahr, dass Marktteilnehmer*innen in unregulierte Marktinfrastrukturen abwandern könnten. Da davon ausgegangen wird, dass die Anonymität den Handel mit Kryptowerten besonders attraktiv macht, müsse damit gerechnet werden, dass Betroffene alternative Lösungen suchen und somit intransparentere Arten von Vermögenstransfers begünstigt würden. Eine derartige Entwicklung würde darüber hinaus eine Schwächung des Anleger*innenschutzes zur Folge haben.

Ein weiterer angesprochener Aspekt bezieht sich auf die Frage des tatsächlichen Missbrauchsrisikos bei Transfers von Kryptowerten. Bitkom hält das Risiko von Geldwäsche und Terrorismusfinanzierung als nicht ausreichend erhoben.⁵¹ Der Wirtschaftsrat der CDU e.V. schätzt den Anteil krimineller Handlungen mittels Kryptowerten als sehr gering ein⁵², Blockchain Bundesverband e.V. sieht gar keine

⁴²Vgl. Bitkom Bundesverband 2021

⁴³Vgl. Blockchain Bundesverband e.V. 2021

⁴⁴Vgl. Die Deutsche Kreditwirtschaft 2021

⁴⁵Vgl. Kapilendo AG 2021

⁴⁶Vgl. Verband der Auslandsbanken in Deutschland e.V. 2021

⁴⁷Vgl. Wirtschaftsrat der CDU e.V. 2021

⁴⁸Vgl. Khayat 2023, 64

⁴⁹Vgl. Bundesverband der Geldwäschebeauftragten e.V. 2021

⁵⁰Vgl. Kapilendo AG 2021

⁵¹Vgl. Bitkom Bundesverband 2021

⁵²Vgl. Wirtschaftsrat der CDU e.V. 2021

Anzeichen dafür, dass Kryptowerte zur Terrorismusfinanzierung eingesetzt werden.⁵³ Darüber hinaus wird in der Stellungnahme der Futurum Bank AG die Treffsicherheit der Verordnung in Bezug auf die Vermeidung illegaler Transaktionen durch ein Nachverfolgen der Transaktionsbeteiligten hinterfragt.⁵⁴ Der Bundesverband der Geldwäschebeauftragten schlägt vor, statt einer automatischen Verpflichtung, eine verstärkte Sorgfaltspflicht nur nach einer entsprechenden Risikoeinschätzung anzuordnen.⁵⁵

Khayat hingegen bewertet die Gefahr kriminellen Einsatzes bei Kryptowertetransfers aufgrund der Anonymität der Beteiligten als in einem Ausmaß gegeben, das eine Erhebung und Verarbeitung von Daten rechtfertigt. Das Ziel der KryptoWTransferV, Geldwäsche und Terrorismusfinanzierung zu verhindern, könnte durch die verstärkten Sorgfaltspflichten erreicht werden. Durch die Verordnung würden jedenfalls jene Transfers geregelt werden, an denen zumindest auf einer Seite ein Kryptowertedienstleister beteiligt ist. Lediglich Transfers, an denen kein Institut beteiligt ist und die Nutzer*innen ausschließlich selbst verwalten (Unhosted Wallets) seien nicht erfasst.⁵⁶

Im Zusammenhang mit der Einschätzung des Missbrauchsrisikos fordert Bitkom, auf die Verhältnismäßigkeit der Maßnahmen zu achten, auch in Bezug auf datenschutzrechtliche Aspekte, da mit der KryptoWTransferV ein starker Eingriff in den Datenschutz und die Geschäftstätigkeit von Finanzdienstleistern unternommen würde.⁵⁷

Datenschutzrechtliche Bedenken werden auch in den Stellungnahmen von Bitkom⁵⁸, der Deutschen Kreditwirtschaft⁵⁹, Kapilendo, vom Verband der Auslandsbanken in Deutschland e.V.⁶⁰ angesprochen. Klarbezeichnungen und Datenübermittlung würden dem Grundprinzip der Pseudonymität widersprechen. Das Sammeln von personenbezogenen Daten ohne Vorliegen klarer Aufbewahrungs- und

⁵³Vgl. Blockchain Bundesverband e.V. 2021

⁵⁴Vgl. Futurum Bank AG 2021

⁵⁵Vgl. Bundesverband der Geldwäschebeauftragten e.V. 2021

⁵⁶Vgl. Khayat 2023, 63

⁵⁷Vgl. Bitkom Bundesverband 2021

⁵⁸Vgl. Bitkom Bundesverband 2021

⁵⁹Vgl. Die Deutsche Kreditwirtschaft 2021

⁶⁰Vgl. Verband der Auslandsbanken in Deutschland e.V. 2021

Verarbeitungsvorschriften wird als datenschutzrechtlich äußerst bedenklich eingeschätzt. Problematisch sei des Weiteren die öffentliche Einsehbarkeit einer Mehrzahl von Blockchain Netzwerken.

4. Verordnung über Märkte für Kryptowerte – (MiCA)

4.1. Zusammenfassung der MiCA-Verordnung

Wie auch schon die Erschaffung der KryptoWTransferV gründet die Entstehung der MiCA-VO im stetig steigenden Interesse der Allgemeinheit an Kryptowerten und vor allem an Kryptowährungen. Während derzeit nicht nur der Handel mit solchen Werten auch unter Privatpersonen boomt, entdecken viele auch die Möglichkeit, mit Kryptowerten Kauftransaktionen durchzuführen. Diese Tatsache war und ist weiterhin der Katalysator für das rasante Wachstum von sogenannten Kryptobörsen wie Kraken, Coinbase, oder auch der österreichischen Variante, Bitpanda. Mit der MiCA-VO soll nun jedoch im Gegensatz zur KryptoWTransferV nicht die Allgemeinheit oder der Staat vor Terrorismusfinanzierung oder Geldwäsche geschützt werden, sondern ist das Hauptziel dieser Verordnung die Regulierung des Marktes per se sowie die Regulierung der an dem Markt teilhabenden Kryptowerte-Dienstleister. Dies ist insbesondere wichtig, da sich bislang ebensolche Dienstleister bis auf einige wenige Ausnahmen in den meisten Mitgliedsstaaten im rechtsfreien Raum bewegt haben, und eine gewisse Regulierung in diesem Bereich im Hinblick auf den Schutz der im Vergleich zu den Kryptowerte-Dienstleistern schwächeren (Privat-)Personen angebracht scheint. Natürlich ist hierbei abermals die Entstehungsgeschichte von Kryptowerten und vor allen Kryptowährungen zu beachten, welche auf einer grundlegenden Dezentralisierung nicht nur der Kryptowerte an sich, sondern auch des ganzen Marktes fußte. Somit begegnete die Legislative im Rahmen der Erlassung der MiCA-VO wiederholt einem gewissen Maß an Gegenwind.

Hierbei darf jedoch nicht aus den Augen gelassen werden, dass ohne den Erlass einer solchen Verordnung einerseits aufgrund von Unsicherheiten bezüglich der rechtlichen Handhabung von Kryptowerten, andererseits aufgrund des Fehlens an einem einheitlichen und abgestimmten Regelungs- und Überwachungssystem in der Europäischen Union, Kryptowerte-Dienstleister und auch -Emittenten mitunter sehr vorsichtig im Umgang mit dem europäischen Krypto-Markt waren. Dies hatte unter anderem die Verzögerung und Verlangsamung von Innovation in der Europäischen Union zur Folge. Durch den Erlass der MiCA-VO soll einer Zersplitterung der Rechtsmaterie durch unterschiedliche nationalstaatliche Regelungen vorgegriffen, und eine durchwegs einheitliche Regulierung geschaffen werden. Hierdurch soll mitunter das Vertrauen der Marktteilnehmer gesteigert werden. Auch soll es

Unternehmen ermöglicht werden, alternative Zahlungsmittel, innovative Digitale Angebote und Dienste sowie auch neue Finanzierungsquellen nutzen zu können. Hierbei steht die Gewährleistung von absoluter Rechtssicherheit im Vordergrund.⁶¹

Auch Privatpersonen und Verbraucher allgemein, sowie Anleger aller Art sollen einen entsprechenden Schutz im bislang quasi rechtsfreien Raum erhalten. Schließlich wird auch ein besonderes Augenmerk auf Transparenz in Bezug auf ihre Rechte und finanzielle Stabilität gelegt.⁶² Somit ist erstreckt sich der persönliche Anwendungsbereich der MiCA-VO gemäß Art 2 Abs 1 MiCA-VO auf sowohl natürliche als auch juristische Personen, die Kryptowerte in der EU ausgeben, öffentlich anbieten, zum Handel freigeben oder Dienstleistungen im Bereich der Kryptowerte erbringen wollen. Dies umfasst insbesondere die bereits erwähnten Emittenten und Kryptowerte-Dienstleister, wie etwa Börsen und Handelsplattformen sowie auch traditionelle Finanzinstitute.⁶³

Die MiCA-VO ist grundsätzlich bereits am 29. Juni 2023 in Kraft getreten. Vollumfänglich tritt die Verordnung gemäß Art 149 Abs 2 MiCA-VO jedoch erst ab dem 30. Dezember 2024 in jedem Mitgliedstaat in Kraft. Die MiCA-VO erfasst Emittenten und Anbieter von Kryptowerten sowie die Erbringer von Krypto-Dienstleistungen (Art. 2 Abs. 1 MiCA-VO). In Art. 3 Abs. 1 Nr. 9 MiCA-VO sind die demnach erfassten Dienstleistungen aufgezählt. Diese umfassen beispielsweise den Betrieb einer Handelsplattform für Kryptowerte oder den Tausch von Kryptowerten gegen Nominalwährungen oder andere Kryptowerte oder die Verwahrung und Verwaltung von Kryptowerten für Dritte.⁶⁴

Wie bereits weiter oben ausführlich dargelegt, lassen sich Kryptowerte in verschiedene Kategorien einteilen. Die MiCA-VO zielt darauf ab, durch Vornahme einer Negativabgrenzung sämtliche Arten von Kryptowerten zu erfassen, die bisher nicht unter das europäische Finanzaufsichtsrecht (wie die MiFID II) fallen.⁶⁵ Kryptowerte, die bereits von anderen europäischen Regelungen abgedeckt sind, sollen vom sachlichen Anwendungsbereich der MiCA-VO ausgeschlossen werden.⁶⁶

⁶¹Vgl. Verordnung (EU) 2023/1114, ErwGr 5

⁶²Vgl. COM(2020) 593 final

⁶³Vgl. Pichler/ Reiterer 2023, 38

⁶⁴Vgl. Europe Direct 2023

⁶⁵Vgl. COM(2020) 593 final, ErwGr 8

⁶⁶Vgl. COM(2020) 593 final, ErwGr 6

Ausgenommen sind demnach gemäß Artikel 2 Abs. 4 lit. a) MiCA-VO zum Beispiel etwa klassische, standardisierte Finanzinstrumente oder gemäß Art 2 Abs 3 der MiCA-VO Kryptowerte, welche eindeutig einzigartig und nicht durch andere Kryptowerte ersetzbar sind.⁶⁷ NFTs bzw. Non-fungible Tokens sind daher vom Geltungsbereich ausgenommen.

Um nun ihre bereits ausführlich dargelegten Ziele zu erreichen, erlegt die MiCA-Verordnung den von ihrem persönlichen Anwendungsbereich betroffenen natürlichen und juristischen Personen verschiedene umfangreiche Anforderungen und Verpflichtungen auf.

4.1.1 Pflichten für Emittenten von Krypto-Werten

Für Emittenten von Kryptowerten bedeutet dies eine Verpflichtung zur Veröffentlichung eines Whitepapers. Art 3 Abs 1 Z 10 MiCA-VO definiert den Begriff „Emittent“ als *„eine natürliche oder juristische Person oder ein anderes Unternehmen, die bzw. das Kryptowerte emittiert“*. In Bezug auf Kryptowerte stellt ein Whitepaper ein Dokument dar, welches vom Emittenten des Kryptowerte-Projekts selbst veröffentlicht wird. Dieses Dokument muss grundsätzlich alle (wichtigen) Informationen im Zusammenhang mit dem Projekt enthalten. Insbesondere sind die Eigenschaften des Kryptowertes zu nennen, sowie die Rechte und Pflichten der künftigen Inhaber. Zwingend müssen auch die Risiken in Bezug auf ein Investment in den Kryptowert enthalten sein. Die obligatorisch im Whitepaper auszuführenden Punkte finden sich für Vermögenswertereferenzierte Token in Art 19 MiCA-VO sowie ausführlicher im Anhang II der MiCA-VO und für E-Geld Token in Art 51 MiCA-VO und ebenfalls detaillierter im Anhang III der MiCA-VO. Eine Auflistung aller in einem Whitepaper verpflichtend enthaltenen Punkte für andere Kryptowerte findet sich in Art 6 MiCA-VO sowie im Anhang I der MiCA-VO⁶⁸. Die Erstellung eines Whitepapers ist allerdings in den in Art 4 Abs 2 und 3 MiCA-VO geregelten Ausnahmefällen nicht zwingend.

Besonders hervorzuheben ist allerdings, dass in Bezug auf vermögenswertereferenzierte Token sowie E-Geld-Token ein höheres Maß an

⁶⁷Vgl. Verordnung (EU) 2023/1114, ErwGr 10

⁶⁸Vgl. Verordnung (EU) 2023/1114, Art 6 Abs 1

Regulierung angewendet wurde und ein zusätzliches, gesondertes Genehmigungsverfahren vorgesehen ist. Die Begründung hierfür liegt in der Natur dieser Kryptowerte. Aufgrund ihrer primären Verwendung als Zahlungsmittel weisen diese Token ein erhöhtes Potenzial für Risiken im Hinblick Marktintegrität und auf Verbraucherschutz auf.⁶⁹ In diesem Zusammenhang gelten für Emittenten auch strengere Kapitalanforderungen, da sie ausreichende Eigenkapitalressourcen und Sicherheiten halten müssen, um den Wert der Token stets zu decken sowie Preisstabilität sicherstellen zu können.

Auch ein erhöhtes Maß an Risikomanagement und Überwachung wird von Emittenten von auf vermögenswertereferenzierte Token verlangt, indem diese robuste Systeme zur Risikobewältigung und sowie auch Überwachungs- und Kontrollmechanismen implementieren müssen, um die wiederum Stabilität der Tokens zu gewährleisten. Handelt es sich beim Emittenten des Kryptowertes allerdings um ein Kreditinstitut, so ist eine gesonderte Genehmigung allerdings nicht erforderlich und müssen auch bedeutend weniger Informationen im Zulassungsverfahren vorgelegt werden.⁷⁰

4.1.2. Pflichten von Krypto-Dienstleistern

Nicht nur die Emittenten von Kryptowerten werden von der MiCA-Verordnung erfasst und reguliert, sondern auch die Anbieter von Dienstleistungen im Zusammenhang mit Kryptowerten. Wie bereits unter 4.2. angeschnitten, handelt es sich hierbei insbesondere um Handelsplattformen (auch Krypto-Börsen genannt), Wallet-Anbieter, Krypto-Verwahrungsdienste, sowie andere Anbieter von Dienstleistungen im Zusammenhang mit dem Tausch von Kryptowerten gegen Fiat-Geld, daher Währungen, die von Regierungen reguliert und kontrolliert werden, oder andere Kryptowerten. Nicht unabsichtlich weisen diese von der MiCA-VO erfassten Kryptowerte-Dienstleistungen eine nicht unübersehbare Similarität zu den Wertpapierdienstleistungen und Anlageaktivitäten der MiFIDII auf.⁷¹

Die meisten dieser Kryptodienstleister unterliegen gemäß Art 63 MiCA-VO nunmehr einer der Pflicht zur Einholung einer separaten Genehmigung, denn um ihre Dienstleistungen anbieten zu dürfen, sind sie verpflichtet, sich bei den hierfür

⁶⁹Vgl. COM(2020) 593 final, ErwG 10 und 25

⁷⁰Vgl. Verordnung (EU) 2023/1114, Art 17

⁷¹Vgl. Richtlinie 2014/65/EU

zuständigen (nationalen) Aufsichtsbehörden zu registrieren und eine Lizenz zu erwerben. Sofern es sich allerdings um ein bereits reguliertes Unternehmen wie zum Beispiel Kreditinstitute oder Verwalter alternativer Investmentfonds handelt, so entfällt eine besondere Zulassungspflicht⁷². Für solche bereits regulierte Unternehmen besteht die Möglichkeit, die Genehmigung zum Anbot ihrer Dienstleistungen im Rahmen eines vereinfachten Verfahrens gemäß Art 60 MiCA-VO zu erlangen.

Kryptowerte-Dienstleister sind gemäß Art 66 MiCA-VO dazu verpflichtet, gewisse, sehr allgemein gehaltene Standards einzuhalten. Dazu zählt allerdings insbesondere, dass sie aufrichtig, fair, professionell und im Interesse ihrer Kunden handeln müssen. Außerdem sind sie verpflichtet, ehrliche, klare und nicht irreführende Kommunikation im Zusammenhang mit den angepriesenen Kryptowert zu gewährleisten sowie vor Risiken im Zusammenhang mit Transaktionen mit Kryptowerten zu warnen.

Schließlich unterliegen Kryptowerte-Dienstleister im Zusammenhang mit ihrer Betriebssicherheit ähnlichen Anforderungen, wie die bereits weiter vorne erläuterten Kryptowerte-Emittenten. Hierzu gehört, dass auch für die Kryptowerte-Dienstleister gewisse Vorschriften zur Unternehmensführung einzuhalten sind, wie das Implementieren von Sicherheitsmaßnahmen, um die sichere Verwahrung von Kryptowerten zu garantieren sowie einen Schutz vor Cyberangriffen zu gewährleisten. Auch sind sie ebenfalls verpflichtet, bestimmten Mindestkapitalanforderungen gerecht zu werden.⁷³ Diese Regelung hat den Hintergrund, dass die Kryptowerte der Kunden im Falle der Insolvenz eines Kryptowerte-Dienstleisters geschützt werden müssen. Nach österreichischem Recht muss daher ein Aus- und Absonderungsrecht der Kunden bestehen.⁷⁴

4.1.3 Rechte von Verbrauchern

Von dem Erlass und Inkrafttreten der VO-VO profitieren direkt und auch indirekt am meisten wohl die Verbraucher. Ihnen wird durch die soeben dargelegten Regelungen ein im Krypto-Raum noch nie dagewesenes Maß an Sicherheit, Aufklärung und Information geboten. Betrugshandlungen im großen Stil und schwerwiegende

⁷²Vgl. Verordnung (EU) 2023/1114, Art 59 Abs 1 lit b

⁷³Vgl. Verordnung (EU) 2023/1114, Art 67, 68

⁷⁴Vgl. Brutkasten / Völkl 2023

sogenannte „Rug-Pulls“, daher betrügerische Manöver, bei dem Emittenten plötzlich alle Mittel aus einem Projekt abziehen und Investoren ohne Wert dastehen lassen, werden zumindest im Geltungsbereich der Verordnung fast gänzlich verhindert.

Verbraucherrechte werden durch die Durchsetzung der soeben erläuterten Transparenzanforderungen sowie insbesondere auch dem Zugang zu detaillierten Informationen über Emittenten sowie Kryptowerte gewährleistet. Auch müssen funktionierende Beschwerdeverfahren eingeführt, um auf Probleme der Verbraucher reagieren zu können. Zudem erfreuen sich die Verbraucher bestimmter besonderer Schutzmechanismen.

Diesbezüglich wird in VO 15 der VO-VO insbesondere eine Haftung des Emittenten zugunsten des Inhabers des Kryptowertes für Schäden verankert, welche aufgrund unvollständiger, unfairer oder nicht eindeutiger Informationsvermittlung im Whitepaper entstehen.⁷⁵

Auch steht den Erwerbern des Kryptowertes ein Widerrufsrecht gemäß VO 13 VO-VO zu, worüber der Erwerber bereits im Whitepaper aufgeklärt werden muss und welches innerhalb von 14 Kalendertagen ab dem Zeitpunkt des Kaufes ausgeübt werden muss. Gemäß VO 13 VO 4 VO-VO gilt ein solches Widerrufsrecht jedoch nicht für Kryptowerte, die zum Beispiel bereits durch einen Kryptowerte-Dienstleister zum Handel zugelassen sind.⁷⁶ Diese Ausnahmeregelung musste in die Verordnung aufgenommen werden, da die Erwerber der Kryptowerte sonst bei einem Kursabsturz die betroffenen Transaktionen widerrufen könnten und hiermit das Grundprinzip des (Krypto-)Handels ausgehebelt würde. Dennoch bedeutet diese Regelung im gleichen Zug auch, dass sie auf die allermeisten Fälle des Erwerbs von zumindest gängigen Kryptowerten nicht anwendbar ist.

4.1.4. Überwachung und Durchsetzung

Die Durchsetzung der MiCA-Verordnung obliegt insbesondere den nationalen Aufsichtsbehörden der einzelnen, jeweiligen EU-Mitgliedstaaten, die in enger und koordinierter Zusammenarbeit mit der Europäischen Bankenaufsichtsbehörde (EBA)

⁷⁵Vgl. Verordnung (EU) 2023/1114, Art 15

⁷⁶Vgl. Verordnung (EU) 2023/1114, Art 13 Abs 4

und der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) handeln. Diese Behörden sind auch für die Überwachung der Einhaltung der Verordnung zuständig und stellen sicher, dass die festgelegten Vorschriften korrekt, in angemessener Zeit und rechtskonform umgesetzt werden. Im Rahmen ihrer Aufgaben überprüfen sie, zusätzlich zu der Überprüfung durch die Krypto-Dienstleister, die von den Emittenten erstellten Whitepapers, um die Transparenz und sowie die Konformität der bereitgestellten Informationen mit der MiCA-VO für Verbraucher zu gewährleisten. Darüber hinaus sind sie für die Lizenzierung von Kryptowerte-Dienstleistern zuständig. Dies ist wichtig, um sicherstellen zu können, dass diese Anbieter die durch die Verordnung gesetzten Standards erfüllen. Im Falle von Verstößen gegen die MiCA-Verordnung, haben ebendiese Aufsichtsbehörden die Befugnis, gewisse Sanktionen zu verhängen, um die Integrität des Krypto-Marktes zu schützen und sicherzustellen, dass die Vorschriften der Verordnung auch weiterhin durchgesetzt werden⁷⁷.

4.2. Begründung für den Erlass der MiCA-Verordnung

Aufgrund der obigen Ausführungen lässt sich bereits feststellen, dass auch der Grund für den Erlass der MiCA-VO der Begründung für den Erlass der KryptoWTransferV sehr ähnelt. Zusammengefasst sollte Rechtssicherheit in einen bisher fast rechtsfreien Raum gebracht werden. Eine solche EU-weite Regelung und Regulierung dieses immer relevanter werdenden Marktes wurde zumindest von den (österreichischen) Behörden bereits sehnsüchtig erwartet, *„da jede Verzögerung der Begleitlegistik zu wesentlicher Rechtsunsicherheit sowohl bei Marktteilnehmern wie auch den involvierten Behörden führt“*⁷⁸.

Zum Beispiel herrschte gerade im Umgang mit Krypto-Werten aufgrund dieser bisherigen Regulierungslücke ein nicht unbedeutendes Machtgefälle zwischen vor allem Emittenten von Krypto-Werten und Verbrauchern. Ohne die Verpflichtung zur Offenlegung von bestimmten Informationen oder zur Hinterlegung von gewissen (monetären) Sicherheiten waren Verbraucher (aber unter Umständen auch Kryptowerte-Dienstleister) oftmals dem Willen der Emittenten ausgeliefert. Diese konnten bislang nach Veröffentlichung eines Krypto-Projektes und nach Erhalt von vielen Investitionen durch vorwiegend Verbraucher oftmals ohne rechtliche

⁷⁷Vgl. Verordnung (EU) 2023/1114

⁷⁸Vgl. Bundesministerium für Finanzen 2024

Konsequenzen, plötzlich alle Geldmittel aus dem Projekt abziehen, wobei die Investoren hiernach oftmals einen Totalverlust der in das Projekt investierten Mittel erleideten und aufgrund der bislang konsequent herrschenden Anonymität in einem Großteil der Fälle auch keine rechtliche Hilfe in Anspruch nehmen konnten. Die MiCA-VO hat es sich jedoch zum Ziel gemacht, mittels einer weitreichenden und einheitlichen Regulierung solche Vorkommnisse zu verhindern und auch grundsätzlich ein hohes Maß an Rechtssicherheit zu schaffen.

Weiters besteht für die grundsätzlich zuständigen Behörden erst ab Schaffung einer gesetzlichen Grundlage die Möglichkeit, nationalen Marktteilnehmern den Zugang zu den nun unionsrechtlich geregelten Märkten für Kryptowerte zu ermöglichen. Die flankierenden behördlichen Befugnisse und Straftatbestände schaffen erst die nötige Grundlage, um einen effektiven Vollzug der Verordnung durch die zuständigen nationalen Behörden zu ermöglichen⁷⁹.

⁷⁹Vgl. Bundesministerium für Finanzen 2024

5. Die EU-Datenschutz-Grundverordnung (DSGVO)

5.1. Allgemeines zur DSGVO

Der Schutz von persönlichen Daten, insbesondere von Privatpersonen, spielte nicht immer eine so große Rolle, wie in der heutigen Zeit. Sowohl die Finanzwelt als auch insbesondere das World Wide Web und somit das Internet an sich haben in den vergangenen zwanzig Jahren eine noch die dagewesene, rasante Entwicklung durchgemacht. Vieles, was am Beginn der zweitausender-Jahre noch unmöglich schien, ist heute durch den technischen Fortschritt der letzten Jahre bereits Realität. Mit all den positiven Veränderungen, die unsere hoch modernisierte Welt nunmehr mit sich bringt, kam jedoch auch die stetig lauende Gefahr des Datenmissbrauchs. Hacks, Scams und Cyber-Angriffe jeglicher Art sind zum Alltag geworden, ermöglicht durch nicht rechtmäßig gesammelte oder nicht ausreichend geschützte personenbezogene Daten. Daten sind nunmehr zu einem dermaßen wichtigen Wirtschaftsgut geworden, dass Unternehmen, sogenannte Daten-Broker, diese an die meistbietenden Käufer verkaufen. Der Schutz und die Kontrolle der eigenen Daten standen daher noch nie mehr im Mittelpunkt, als heute. Insbesondere in den letzten zehn Jahren erkannte man daher die Wichtigkeit des Datenschutzes und arbeitete man an Möglichkeiten, den Datenschutz auch rechtlich besser zu verankern.

Die Entstehung der Datenschutz-Grundverordnung ist das Resultat eines äußerst langwierigen und komplexen Prozesses, der durch das wachsende Bedürfnis nach einem modernen, umfassenden, rechtlichen Datenschutzrahmen innerhalb der Europäischen Union ausgelöst wurde. Insbesondere die Richtlinie 95/46/EG⁸⁰, welche die Grundlage des europäischen Datenschutzes seit den 1990er Jahren bildete und erst 2018 durch die DSGVO abgelöst wurde, war angesichts der rasant fortschreitenden technischen Entwicklungen, insbesondere des Internets, und der globalisierten Wirtschaft nicht mehr zeitgemäß. Die treibende Kraft hinter der DSGVO war daher das Bedürfnis, eine einheitliche und kohärente Rechtsgrundlage für den Datenschutz in allen EU-Mitgliedstaaten zu schaffen. Ein weiteres zentrales Anliegen war der Schutz der Privatsphäre der Bürger der EU-Mitgliedsstaaten, welche durch die zunehmende Digitalisierung und die steigende Menge an verarbeiteten personenbezogenen Daten immer stärker bedroht wurde.

⁸⁰Vgl. Richtlinie 95/46/EG

Dieses Kapitel dient dazu, einen Überblick über die Betroffenenrechte gemäß der EU-Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, bieten. Diese trat am 24. Mai 2016 in Kraft und findet seit 25. Mai 2018 in der gesamten EU verbindlich Anwendung.⁸¹ Seit dieser Zeit haben sich viele Regelungen verändert, sind neue Pflichten geschaffen und Bußgelder bei deren Verletzung wesentlich erhöht worden und ist die Bedeutung des Datenschutzrechts insgesamt stark gestiegen. Die neue DSGVO hatte nicht zuletzt das Ziel, einen sensibleren Umgang mit personenbezogenen Daten herbeizuführen.⁸² Die DSGVO verfolgt dabei zwei Schutzziele: Einerseits soll die Privatsphäre der betroffenen Person, deren Daten erhoben und verarbeitet werden, gewahrt und eine missbräuchliche Verwendung der Daten verhindert werden. Gleichzeitig soll aber der freie Datenverkehr ermöglicht werden. Um eine für den grenzüberschreitenden Datenaustausch nötige weitgehende Vereinheitlichung der Datenschutzrichtlinien in den EU-Mitgliedstaaten zu erreichen, wurde die DSGVO erlassen. Allerdings lässt die DSGVO durch Öffnungsklauseln Spielräume für nationale Regelungen offen.⁸³ In Österreich sind die Maßnahmen zum Datenschutz in Bezug auf nationale Durchführungs- und Anpassungsbestimmungen im Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG) reguliert.⁸⁴

In der Charta der Grundrechte der Europäischen Union (GRC) soll durch den Artikel 8 der Schutz personenbezogener Daten garantiert werden.⁸⁵ Somit bilden Artikel 8 und Artikel 7 der GRC, in dem ein Recht auf Achtung des Privatlebens festgelegt wird, die Basis für die DSGVO.⁸⁶

5.2. Zusammenfassung der Betroffenenrechte in der DSGVO

Die Betroffenenrechte sind in der DSGVO unter den Artikeln 12 bis 23 geregelt.

Die festgelegten Rechte beziehen sich auf die Bereiche Transparenz, Information,

⁸¹Vgl. Bergauer / Jahnel (Hrsg.) 2018, V

⁸²Vgl. Jahnel / Pallwein-Prettner 2021, 5f.

⁸³Vgl. Jahnel / Pallwein-Prettner 2021, 15f.

⁸⁴Vgl. Bergauer / Jahnel (Hrsg.) 2018, V

⁸⁵Vgl. Bergauer / Jahnel (Hrsg.) 2018, 5ff.

⁸⁶Vgl. Jahnel / Pallwein-Prettner 2021, 29

Berichtigung, Löschung und Widerspruch und können überblicksmäßig wie folgt zusammengefasst werden.

Transparenz und Modalitäten (Artikel 12)

Der betroffenen Person müssen Informationen über die Verarbeitung ihrer Daten klar, verständlich und grundsätzlich unentgeltlich zur Verfügung gestellt und durch entsprechende Modalitäten der Zugang zur Wahrnehmung ihrer Rechte erleichtert werden.⁸⁷

Informationspflicht und Recht auf Auskunft (Artikel 13 bis 15)

Betroffene Personen sind bei der Erhebung ihrer Daten über bestimmte Fakten aufzuklären (es sei denn, genau definierte Ausnahmegründe sprechen dagegen). Dies beinhaltet Informationen über den „Verantwortlichen“⁸⁸, den Verarbeitungszweck, die Rechtsgrundlage, die Empfänger*innen, die Speicherdauer und die Rechte der betroffenen Person, sowie die Auskunft, ob sie verpflichtet ist, die Daten bereit zu stellen. Im Fall, dass personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, sind ihr die Informationen, inkl. der Bekanntgabe, aus welcher Quelle die Daten stammen, innerhalb einer angemessenen Frist (längstens innerhalb eines Monats) mitzuteilen. Neben der Informationspflicht durch die Verantwortlichen, besteht das Recht auf Auskunft für betroffene Personen. Diese haben u.a. das Recht, eine Bestätigung zu erhalten, ob und welche sie betreffende personenbezogene Daten verarbeitet werden. Ferner können sie Zugang zu diesen Daten, sowie weitere Informationen beispielsweise über Verarbeitungszweck, Empfänger*innen und Speicherdauer verlangen und Aufklärung über ihre Rechte (wie das auf Berichtigung, Löschung, Einschränkung etc.) fordern.⁸⁹

Berichtigung, Löschung und Einschränkung (Artikel 16 bis 20)

Die betroffene Person hat das Recht, unrichtige Daten unverzüglich berichtigen und unvollständige Daten ergänzen zu lassen. Das Recht auf Löschung, das „Recht auf

⁸⁷Vgl. Bergauer / Jahnel (Hrsg.) 2018, 73ff.

⁸⁸Unter „Verantwortlicher“ ist laut Begriffsbestimmung gem. Artikel 4 DSGVO eine natürliche oder juristische Person zu verstehen, die über die Verarbeitung von personenbezogenen Daten entscheidet. Vgl. Bergauer / Jahnel (Hrsg.) 2018, 31

⁸⁹Vgl. Bergauer / Jahnel (Hrsg.) 2018, 76ff.

Vergessenwerden“, findet unter gewissen Bedingungen bei Vorliegen von in der Verordnung definierten Gründen Anwendung. Beispielfhaft können folgende Gründe genannt werden: die Speicherung der Daten für die ursprünglichen Verarbeitungszwecke ist nicht mehr erforderlich, die Verarbeitung unrechtmäßig, eine Einwilligung wurde widerrufen oder ein Widerspruch eingelegt. Ferner ist der Verantwortliche, der personenbezogene Daten öffentlich gemacht hat, verpflichtet, die für die Verarbeitung Verantwortlichen über einen etwaigen Antrag auf Löschung aller Links zu diesen Daten zu informieren. Das Recht auf Löschung gilt nur unter bestimmten Umständen nicht, zum Beispiel, wenn die Verarbeitung von Daten zur Ausübung der freien Meinungsäußerung erforderlich ist oder die weitere Speicherung im öffentlichen Interesse liegt, wissenschaftlichen oder historischen Forschungszwecken dient. Die betroffene Person hat in bestimmten Fällen das Recht auf Einschränkung der Verarbeitung ihrer Daten. Demnach dürfen Daten nur begrenzt verarbeitet werden, wenn die Richtigkeit bestritten wird oder die Verarbeitung unrechtmäßig ist (aber die Löschung nicht verlangt wird), wenn die betroffene Person die Daten für gewisse Zwecke benötigt aber der Verantwortliche nicht mehr, oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, aber noch keine Entscheidung darüber getroffen wurde. Der Verantwortliche hat den Empfänger*innen jede Berichtigung, Löschung oder Einschränkung mitzuteilen (mit der Ausnahme der Unmöglichkeit oder Unverhältnismäßigkeit). Die betroffene Person kann Auskunft über die Empfänger*innen verlangen. Die betroffene Person hat das Recht auf Datenübertragbarkeit, also das Recht, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln.⁹⁰

Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall (Artikel 21 und 22)

Die betroffene Person hat das Recht gegen die Verarbeitung ihrer Daten Widerspruch einzulegen. Der Verantwortliche darf die Daten nur weiterverarbeiten, wenn er zwingende schutzwürdige Gründe nachweisen kann. Betreffen die Verarbeitungszwecke eine Direktwerbung, hat die betroffene Person jederzeit das Recht Widerspruch einzulegen und die Daten dürfen dazu nicht mehr verarbeitet werden. Über diese Rechte ist die betroffene Person ausdrücklich und in

⁹⁰Vgl. Bergauer / Jahnel (Hrsg.) 2018, 87ff.

verständlicher Form aufzuklären. Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden ohne Möglichkeit menschlichen Eingreifens, sofern dies rechtliche Wirkung oder erhebliche Beeinträchtigung zur Folge hat. Als Ausnahmegründe werden Situationen angeführt, in welchen die Entscheidung für Abschluss oder Erfüllung eines Vertrags erforderlich ist. Dies aufgrund von Rechtsvorschriften der Union oder derer Mitgliedstaaten, denen der Verantwortliche unterliegt, sowie schließlich, wenn die betroffene Person ihre Einwilligung erteilt.⁹¹

Beschränkungen (Artikel 23)

Durch Rechtsvorschriften der Union oder der Mitgliedstaaten können, wenn sie spezifische Bestimmungen beinhalten, die oben beschriebene Pflichten und Rechte beschränkt werden. Dies, sofern eine solche Einschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist um gewisse Umstände sicherzustellen, wie etwa die Aufrechterhaltung der nationalen und öffentlichen Sicherheit sowie die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Ferner ist eine Beschränkung der bereits ausgeführten Rechte und Pflichten dann erforderlich, wenn es um den Schutz einer betroffenen Person oder die Rechte und Freiheiten anderer Personen geht, um einige Aspekte beispielhaft aufzuzählen.⁹²

⁹¹Vgl. Bergauer / Jahnel (Hrsg.) 2018, 97ff.

⁹²Vgl. Bergauer / Jahnel (Hrsg.) 2018, 102ff.

6. Transparenz versus Schutz von Daten

6.1. Analyse der Vereinbarkeit DSGVO und KryptoWTransferV

Dem Schutz von insbesondere personenbezogenen Daten sowie der Betroffenenrechte gemäß DSGVO kommt in der heutigen Gesellschaft ein besonders hoher Stellenwert zu. Sieht man das Internet als ein riesengroßes Netzwerk an für immer gespeicherten Daten, so fällt es nicht schwer zu verstehen, wieso der Ruf nach Gewährung eines bestimmten Maßes der Sicherheit der persönlichen Daten sowie die Einhaltung der Betroffenenrechte einer jeden Person immer unüberhörbarer wird. Durch unter anderem stets öfter vorkommende Hackerangriffe und hiernach folgenden Identitätsdiebstählen oder betrügerischen Handlungen sowie auch durch die kontinuierlich stärker werdende Kontrolle durch Behörden werden jene Stimmen konstant lauter, welche eine fast durchwegs anonymisierte Bewegungsfreiheit einer jeden Person im Internet fordern. Diese Unabhängigkeit von den zentralisierten Kontrollmaßnahmen staatlicher Regierungen war, wie bereits in früheren Kapiteln erwähnt, ein starker Treiber für die Erschaffung von Kryptowerten und Kryptowährungen.

Dem entgegensteht jedoch die Devise, dass das Internet kein rechtsfreier Raum ist und auch nicht zu einem solchen werden darf. Insbesondere beim Umgang mit Geld- oder Kryptowerten besteht das Interesse aber auch die Verpflichtung eines jeden Staates, kriminelle Machenschaften jeglicher Art zu Unterbinden.

Hierdurch entsteht das Paradoxon „Transparenz versus Schutz von (personenbezogenen)“ Daten. Es muss der bestmögliche Schutz von (insbesondere sensiblen) Daten gewährleistet werden, im gleichen Zug allerdings auch eine gewisse Kontrolle der betroffenen Behörden bzw. staatlichen Einrichtungen ermöglicht werden, um hierdurch insbesondere die Erschaffung eines rechtsfreien Raumes abzuwenden und im gleichen Zug auch die Verhinderung und Verfolgung von Straftaten und insbesondere von Terrorismusfinanzierung zu gewährleisten. Die bereits näher umschriebene DSGVO versucht sich an der Meistung dieser Gratwanderung.

Wie bereits etwas ausführlicher dargelegt, zielt die KryptoWTransferV im Gegenzug jedoch auf die Verhinderung von Geldwäsche und Terrorismusfinanzierung ab, indem sie die Übertragung von Kryptowerten regelt und vor allem reguliert.

In Bezug auf die Betroffenenrechte der DSGVO (insbesondere das Auskunftsrecht, das Recht auf Löschung, das Recht auf Berichtigung und das Widerspruchsrecht), welche sich in den Artikeln 12 bis 23 finden lassen, entsteht im Rahmen der KryptoWTransferV ein Spannungsverhältnis, insbesondere im Hinblick auf die Notwendigkeit der Datenspeicherung und -weitergabe im Rahmen der KryptoWTransferV sowie den eben genannten Betroffenenrechten der DSGVO. Dies, da die KryptoWTransferV die Erfassung und Weitergabe von personenbezogenen Daten verlangt, um hierdurch ihr Ziel verwirklichen zu können, nämlich die Nachverfolgbarkeit von Kryptotransaktionen gewährleisten zu können. Hieraus ergeben sich grundlegend unterschiedliche Zielsetzungen der beiden Normen.

Um diesen Interessenskonflikt bewältigen zu können, kann jedoch auf bestimmte Mechanismen der DSGVO zurückgegriffen werden:

Datenminimierung, Zweckbindung und Verhältnismäßigkeit

Die Minimierung der Menge an Daten, welche verarbeitet werden sowie auch die Verhältnismäßigkeit der Verarbeitung von Daten gehören zu den Grundprinzipien der DSGVO, welche auch trotz der Einschränkungen durch die KryptoWTransferV gewahrt werden müssen. Das Gebot der Datenminimierung findet sich in Artikel 5 der DSGVO. In der Praxis bedeutet dies, dass nur die für den Zweck notwendigen (Transaktions)Daten erhoben und sodann auch verarbeitet werden dürfen. Daten, welche nicht unbedingt notwendig zur Einhaltung der KryptoWTransferV sind, dürfen weder erhoben noch verarbeitet werden. Die rechtmäßig erhobenen und verarbeiteten Daten dürfen auch nur so lange gespeichert werden, wie dies notwendig ist, um im Einklang mit der KryptoWTransferV zu stehen. Mehr Informationen als zur Erfüllung der Vorschriften der KryptoWTransferV notwendig, dürfen nicht gesammelt werden. Schließlich dürfen die erhobenen Daten auch nur im Rahmen der Verhinderung von Geldwäsche und Terrorismusfinanzierung verwendet werden. Sofern die betroffene Person keine Einwilligung hierzu erteilt hat, dürfen die personenbezogenen Daten zu anderen Zwecken daher nicht verwendet werden.

Rechtmäßigkeit der Datenverarbeitung

Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten kann, um die grundlegende Wahrung von Betroffenenrechten im gesetzlichen Rahmen gewährleisten zu können, auch auf Artikel 6 Abs 1 lit. c DSGVO gestützt werden. Diese Regelung besagt, dass die Datenverarbeitung insbesondere dann gerechtfertigt ist, wenn sie im Rahmen der Erfüllung einer rechtlichen Verpflichtung geschieht. Die KryptoWTransferV stellt eine genau solche rechtliche Verpflichtung dar, welche von den durchführenden Dienstleistern geachtet und befolgt werden muss. Die grundsätzliche Rechtmäßigkeit der Datenverarbeitung ist daher schon aufgrund der rechtlich bindenden Wirkung der KryptoWTransferV gegeben.

Transparenz über die Verarbeitung von Daten

Artikel 13 und 14 der DSGVO normieren, dass betroffene Personen über die Erhebung und Verarbeitung ihrer Daten verpflichtend durch die verarbeitenden Dienstleister zu informieren sind. Diese Informationspflicht schließt insbesondere Informationen darüber ein, welche Daten genau erhoben werden, für welche Dauer diese Daten gespeichert werden und in welchem Rahmen beziehungsweise zu welchem Zweck die Verarbeitung dieser Daten erfolgt. Sofern die personenbezogenen Daten nicht bei der betroffenen Person selbst erhoben werden, so muss ebenfalls darüber aufgeklärt werden, aus welcher Quelle die Daten stammen und ob es sich hierbei um öffentlich zugängliche Quellen handelt. Darüber hinaus besteht unter anderem auch die Verpflichtung zur Aufklärung über bestimmte Beschwerderechte.

Einschränkungen von Betroffenenrechten

Sofern eine rechtliche Verpflichtung zur Datenverarbeitung besteht, wie dies insbesondere auch in der KryptoWTransferV der Fall ist, so können bestimmte Betroffenenrechte, wie das Widerspruchsrecht oder das Recht auf Löschung gegebenenfalls eingeschränkt werden. Die DSGVO normiert jedoch, dass ebensolche Betroffenenrechte nur in einem solchen Maße eingeschränkt werden dürfen, wie dies zur Erfüllung der rechtlichen Anforderungen nötig ist. Eine hierüber hinausgehende Einschränkung der Betroffenenrechte ist jedenfalls zu unterlassen.

Es ist somit festzuhalten, dass auch im Zusammenhang mit der KryptoWTransferV weiterhin eine gewisse grundlegende Wahrung der Betroffenenrechte gewährleistet wird. Aufgrund der spezifischen Anforderungen der gegenständlichen Norm unterliegen Betroffenenrechte jedoch klar definierten und regulierten Einschränkungen. Solche Einschränkungen sind insbesondere dann rechtlich unbedenklich, wenn sie auf der Erfüllung einer gesetzlichen Verpflichtung beruhen und die Prinzipien der Verhältnismäßigkeit und Datenminimierung gewahrt bleiben.

6.2. Analyse der Vereinbarkeit DSGVO und MiCA-VO

Wie bereits ausführlich dargelegt, regelt die MiCA-Verordnung die Emission und auch den Handel von Krypto-Werten innerhalb der Europäischen Union. Hierbei zielt sie hauptsächlich darauf ab, Verbraucher zu schützen und einen einheitlichen rechtlichen Rahmen für den Krypto-Sektor zu schaffen. Dennoch spielt gleichzeitig auch der Datenschutz eine zentrale Rolle und wird durch die DSGVO-Konformität der MiCA-VO gewährleistet. Hierbei wird insbesondere auf den Schutz der personenbezogenen Daten von Nutzern, Anlegern und Marktteilnehmern überhaupt geachtet.

Dennoch scheint die Existenz beider Verordnungen nebeneinander, eingangs sehr paradox, denn verfolgen die MiCA-Verordnung und die DSGVO unterschiedliche, teilweise sogar konkurrierende Ziele. Während die MiCA-VO zum Ziel hat, insbesondere Transparenz und Stabilität in den Märkten für Krypto-Werte zu schaffen sowie zusammen mit der KryptoWTransferV Geldwäsche und Terrorismusfinanzierung zu verhindern, soll die DSGVO den Schutz personenbezogener Daten und die Gewährleistung von Betroffenenrechten sicherstellen. Da die MiCA-VO hohe Transparenz- sowie Informationsanforderungen verlangt und hierbei unumgänglich Massen an personenbezogenen Daten verarbeitet werden, entsteht auch hier, ähnlich wie bei der KryptoWTransferV, ein potenzieller Konflikt zwischen der Verordnung und der DSGVO.

Besonders stark zeigt sich dieser potenzielle Konflikt in Bezug auf Krypto-Dienstleister, denn die MiCA-VO fordert von Kryptowerte-Dienstleistern eine nicht unerhebliche Transparenz in Bezug auf die Identifikation von Nutzern und die getätigten Transaktionen. Dies betrifft insbesondere Dienstleister wie Handelsplattformen oder Krypto-Wallet-Anbieter, welche Daten über jene Personen, die Krypto-Werte kaufen,

verkaufen oder halten, sammeln und verarbeiten müssen. Hierzu gehören deren Identifikationsdaten wie Name, Adresse und Geburtsdatum, aber auch Transaktionsdetails und Informationen über die Beteiligung an bestimmten Token-Emissionen oder Handelstransaktionen.

Diese Regelungen im Hinblick auf den Umgang mit den eben beschriebenen Daten entsprechen weitestgehend den Vorgaben zur Bekämpfung von Terrorismusfinanzierung und Geldwäsche und insbesondere auch den Regelungen der KryptoWTransferV. Auch die MiCA-VO kann als eine rechtliche Verpflichtung betrachtet werden, welche gemäß Art. 6 Abs. 1 lit. c ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Erfüllung dieser rechtlichen Verpflichtung erforderlich ist.

Wie bereits im Zusammenhang mit der KryptoWTransferV festgestellt, ist ein wichtiger Aspekt in der DSGVO ist die Möglichkeit der Einschränkung bestimmter Betroffenenrechte, sofern ein übergeordnetes öffentliches Interesse besteht. Sowohl die MiCA-Verordnung als auch die KryptoWTransferV erfüllen dieses Kriterium, wenn sie den Eingriff in Betroffenenrechte Verlangen. Diesbezüglich ist das Ziel der MiCA-VO die Gewährleistung von Sicherheit und Marktstabilität. Angesichts der Risiken, die mit dem Umgang mit Krypto-Werten verbunden sind und sich im Zusammenhang mit der MiCA-VO nicht nur auch durch mögliche Terrorismusfinanzierung und Geldwäsche, sondern auch Marktmanipulation sowie die Schädigung von Verbrauchern äußern kann, ist die Durchsetzung strenger Transparenz- und Offenlegungspflichten unvermeidlich. In dieser Hinsicht können die Einschränkungen der Betroffenenrechte jedenfalls als verhältnismäßig und rechtmäßig angesehen werden.

Jedoch müssen auch bei der Umsetzung der MiCA-Verordnung die Datenschutzgrundsätze der DSGVO, wie etwa die Datenminimierung, Zweckbindung und Speicherbegrenzung, geachtet und implementiert werden. Das bedeutet zum Beispiel für Krypto-Dienstleister konkret, dass nur die für die Erfüllung der regulatorischen Pflichten notwendigen Daten erheben und verarbeiten dürfen.

Auch die MiCA-VO muss sich an die weiter oben bereits ausführlicher erläuterten Grundsätze der Datenminimierung und Speicherbegrenzung, Zweckbindung und

Verhältnismäßigkeit gemäß Artikel 5 der DSGVO, der Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 6 Abs 1 lit. c DSGVO sowie der Transparenz über die Verarbeitung von Daten gemäß Artikel 13 und 14 der DSGVO halten. Hierbei wird auf die Ausführungen in Punkt 6.1 verwiesen, um eine Redundanz zu vermeiden.

Diese Grundsätze sollen zusammengefasst sicherstellen, dass nur die tatsächlich erforderlichen Daten für klar definierte Zwecke rechtmäßig erhoben und verarbeitet werden, wobei die Verarbeitung stets in einem angemessenen Verhältnis zum verfolgten Zweck stehen muss und die Daten nur für einen bestimmten Zeitraum gespeichert werden dürfen. Die Anforderungen an Transparenz über die Verarbeitung von Daten stellen zudem sicher, dass betroffene Personen umfassend über Art, Umfang und Zweck der Datenverarbeitung informiert werden. Hierdurch wird eine gewisse Kontrolle über die eigenen Daten gewährleistet.

Ein besonderes Augenmerk muss im Rahmen der Überprüfung der Konformität der MiCA-VO mit der DSGVO auf das Recht der Datenübertragbarkeit gemäß Artikel 20 DSGVO. Diese Bestimmung ist für betroffene Personen insbesondere dann relevant, wenn sie etwa ihren Krypto-Dienstleister wechseln möchten. Zwar beeinträchtigt die MiCA-VO dieses Recht nicht direkt, jedoch muss diesbezüglich – wenn Daten von einem Anbieter auf den anderen übertragen werden – sichergestellt werden, dass der zukünftige Dienstleister dieselben Datenschutzstandards erfüllt, wie der bisherige Verantwortliche. Ist dieses Kriterium erfüllt, so hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.⁹³

Zudem ist auch hervorzuheben, dass die MiCA-VO im Einklang mit der DSGVO von Krypto-Dienstleistern fordert, geeignete technische und organisatorische Maßnahmen zu implementieren. Dies hat einen besonders hohen Stellenwert im Rahmen der Gewährleistung der Sicherheit der erhobenen und verarbeiteten Daten. Die diesbezüglichen Anforderungen der MiCA-VO sind deckungsgleich mit den Regelungen und Regelungen der DSGVO und spielen hierbei insbesondere der

⁹³Vgl. Verordnung (EU) 2016/679

Schutz der Integrität, Verfügbarkeit und Vertraulichkeit personenbezogener Daten eine bedeutende Rolle. Um dies gewährleisten zu können, wird auch im Rahmen der MiCA-VO – wie von der DSGVO gefordert – unter anderem auf die Verschlüsselung von Daten, Zugriffskontrollen und Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO gesetzt.

Abschließend lässt sich somit festhalten, dass sowohl die MiCA-Verordnung als auch die KryptoWTansferV zwangsläufig in die – in der DSGVO verankerten – Betroffenenrechte eingreifen. Dies ist insbesondere bei Rechten wie dem Recht auf Anonymität, Löschung und Transparenz der Fall. Dennoch bleiben diese Eingriffe und Einschränkungen in einem rechtlich zulässigen Rahmen und sind zur Erreichung höherer Ziele wie der Verhinderung illegaler Aktivitäten und der Stabilisierung der Finanzmärkte notwendig.

Die Gratwanderung zwischen Eingriffen in die Rechte der betroffenen Personen und den regulatorischen Erfordernissen des Krypto-Sektors schaffen grundsätzlich sowohl die MiCA-VO als auch die KryptoWTansferV. Dies, obwohl es in der Praxis im Rahmen der Anwendung, Umsetzung und Durchsetzung beider Verordnungen weiterhin zu Spannungen kommen kann.

Langfristig bleibt abzuwarten, ob die MiCA-VO und die KryptoWTansferV zu Anpassungen der DSGVO oder einer weiteren Differenzierung der Betroffenenrechte im Kontext neuer Technologien führen werden. In jedem Fall war die Entstehung beider Verordnungen entscheidend und bahnbrechend, da hierdurch ein angemessener Ausgleich zwischen der Wahrung der Privatsphäre und der Sicherstellung eines transparenten und sicheren Marktes gefunden werden konnte, um den Krypto-Markt nachhaltig und zukunftsfähig zu gestalten.

6.3. Exkurs - EuGH Urteil zur Unvereinbarkeit der EU-Geldwäscherichtlinie mit der GRC

Bereits in den Stellungnahmen zum Referentenentwurf der KryptoWTransferV wurden, wie in Kapitel 3.3 beschrieben, Bedenken zur Vereinbarkeit dieser mit datenschutzrechtlichen Bestimmungen erwähnt. Oben beschriebene Betroffenenrechte sollen den Schutz der Privatsphäre gewährleisten und eine missbräuchliche Verwendung der Daten verhindern, während die KryptoWTransferV darauf abzielt, Kryptowertetransfers zur Nutzung krimineller Aktivitäten unattraktiv zu machen, indem ein gewisses Maß an Transparenz vorgeschrieben wird.

Mit diesem Spannungsfeld „Transparenz versus Schutz der Privatsphäre und Schutz personenbezogener Daten“ hat sich der Europäische Gerichtshof, im Folgenden EuGH genannt, aufgrund der Klage einer luxemburgischen Gesellschaft und deren wirtschaftlichen Eigentümers, beschäftigt. In diesem Fall ging es um eine Unvereinbarkeit der EU-Geldwäscherichtlinie mit der GRC.⁹⁴

Im luxemburgischen Transparenzregister wurden gemäß der Geldwäscherichtlinie personenbezogene Daten über wirtschaftliche Eigentümer*innen eingegeben und teilweise der Öffentlichkeit zugänglich gemacht. Eine Gesellschaft und deren wirtschaftlicher Eigentümer brachten eine Klage ein, um die Rechte auf Einsichtnahme durch die Öffentlichkeit einzuschränken. Tatsächlich hat der EuGH mit Urteil vom 22. November 2022 Teile der EU-Geldwäscherichtlinie für nicht gültig erklärt.⁹⁵

Der EuGH stellte fest, dass die öffentliche Einsichtnahme einen schweren Eingriff in die Grundrechte auf Achtung des Privat- und Familienlebens (Art. 7 GRC) und Schutz personenbezogener Daten (Art. 8 GRC) darstellt.⁹⁶

Konkret wird jene Bestimmung als unvereinbar mit der GRC gesehen, welche besagt, dass eine uneingeschränkte Einsichtnahme in das Transparenzregister jederzeit gegeben sein muss. Das Transparenzregister ist ein öffentliches Register. Jede Person, die sich online registriert, kann dieses Register einsehen und zu fast allen

⁹⁴Vgl. Reißler 2022

⁹⁵Vgl. Reißler 2022

⁹⁶Vgl. Richter et al. 2022

erfassten Daten Zugang erhalten. Gesellschaften mit Sitz in Deutschland müssen ihre (fiktiv) wirtschaftlichen Berechtigten eintragen und personenbezogene Daten bekanntgeben, nämlich Vor- und Nachname, Geburtsdatum, Wohnort, Staatsangehörigkeit, Art und Umfang des wirtschaftlichen Interesses. All diese Daten, ausgenommen Geburtsdatum und Wohnort, können abgerufen werden. Es besteht die Gefahr, dass diese veröffentlichten Daten sodann missbräuchlich gespeichert und verarbeitet werden könnten.⁹⁷

Aufgrund dieses uneingeschränkten Zugangs zu den personenbezogenen Informationen wird dieser Teil vom EuGH als rechtswidrig erklärt, weil dieser schwerwiegende Eingriff in die Grundrechte gem. Art. 7 und Art. 8 GRC nicht auf das absolut Erforderliche beschränkt ist und unverhältnismäßig in Hinblick auf das Ziel der Verhinderung von Geldwäsche und Terrorismusfinanzierung ist.⁹⁸

⁹⁷Vgl. Reißler 2022

⁹⁸Vgl. Reißler 2022

7. Conclusio

Abschließend lässt sich sagen, dass die Betroffenenrechte nach der DSGVO sowohl in der Kryptowertetransferverordnung als auch in der MiCA-Verordnung bestmöglich gewahrt bleiben. Die DSGVO sieht zwangsläufig eine Vielzahl an Ausnahmebestimmungen und Regelungen vor, die eine Verarbeitung personenbezogener Daten unter streng definierten Bedingungen erlauben, auch wenn diese in einem die Grundbestimmungen der DSGVO übersteigenden Ausmaß erfolgt. Diese Ausnahmebestimmungen sind erforderlich, um die effektive Umsetzung regulatorischer Verpflichtungen zu gewährleisten, insbesondere im Hinblick auf die Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie den Schutz von Verbrauchern und des Krypto-Marktes als Ganzes.

Die MiCA-Verordnung und die Kryptowertetransferverordnung setzen auf eine umfassende Erfassung als auch Verarbeitung von Daten und steht dies in einem Spannungsverhältnis zu dem Schutz der Betroffenenrechte. Es ist jedoch hervorzuheben, dass ohne die Ausnahmeregelungen der DSGVO, welche in bestimmten Fällen den Eingriff in die Betroffenenrechte erlaubt, eine effektive Durchsetzung der Kryptowertetransferverordnung sowie der MiCA-Verordnung praktisch kaum möglich wäre. Ohne eine solche, doch relativ weitreichende Flexibilität in den Datenschutzvorgaben könnte die regulatorische Kontrolle und Überwachung des Krypto-Markts nicht in dem notwendigen Umfang gewährleistet werden, was wiederum zu erheblichen Sicherheitsrisiken für alle Beteiligten führen könnte.

Beide Verordnungen stützen sich in hohem Maße auf die Erhebung und Verarbeitung personenbezogener Daten, was die Betroffenenrechte einer jeden Person, die eine Transaktion im Krypto-Raum durchführt, erheblich einschränkt. Dies betrifft insbesondere die Rechte auf Transparenz, Löschung aber auch Auskunft, welche durch die Notwendigkeit zur Erfüllung regulatorischer Verpflichtungen in einigen Fällen stark eingeschränkt oder sogar ganz ausgehebelt werden können.

Gleichzeitig ist es wichtig, das große Potenzial im Auge zu behalten, welches die Verordnungen für die Zukunft der Finanzmärkte in Europa beherbergen. Die umfassende Regulierung durch die MiCA-Verordnung schafft Vertrauen in den Markt für Krypto-Werte und sorgt dafür, dass sowohl institutionelle als auch private Anleger stärker geschützt sind.

Die Kritik, welche hiermit einhergeht, ist, dass Krypto-Werte stark auf dem Argument der Anonymisierung und der Dezentralisierung aufbauen. Genau diese Eigenschaften sind es, die insbesondere Kryptowährungen ihre heutzutage sicherlich als hoch einzustufende Beliebtheit ermöglicht haben. Die Natur der Blockchain-Technologie, die auf einem dezentralen Netzwerk basiert und dem pseudonymen Charakter vieler Kryptowährungen, ermöglicht es Nutzern, Transaktionen ohne die Einbeziehung traditioneller Finanzinstitutionen durchzuführen. Diese Eigenschaften stehen jedoch im Widerspruch zu den Interessen der Regulierungsbehörden, die auf Transparenz und Nachverfolgbarkeit bestehen, um illegale Aktivitäten jeglicher Art zu verhindern.

Ebendiese hohe Anonymität und die hieraus folgenden zahlreichen Zwischenfälle der vergangenen Jahre haben nunmehr die durch die KryptoWTransferV und MiCA-VO erfolgte staatenübergreifende Regelung unumgänglich. Fälle von Geldwäsche, Terrorismusfinanzierung und anderen illegalen Aktivitäten im Zusammenhang mit Kryptowährungen haben gezeigt, dass eine fehlende Regulierung erhebliche Risiken nicht nur auf privater oder unternehmenstechnischer, sondern auch auf staatlicher Ebene birgt. Es wurde erkannt, dass Kryptowährungen ohne angemessene Regulierungsmechanismen ein potenzielles und nicht unerhebliches Sicherheitsrisiko darstellen können.

Führt man daher eine Interessenabwägung zwischen dem Schutz der Betroffenenrechte und der Bewahrung der Anonymität im Krypto-Sektor auf der einen Seite, sowie der Sicherstellung eines stabilen und sicheren Krypto-Marktes auf der anderen Seite durch, so zeigt sich, dass jeglicher Eingriff in die Rechte der Betroffenen, solange er im Rahmen der genannten Verordnungen rechtmäßig erfolgt, gerechtfertigt erscheint.

In Anbetracht der wachsenden Bedeutung von Krypto-Werten jeglicher Art für den globalen Finanzmarkt ist es unabdingbar, dass diese Märkte nicht nur stabil, sondern auch sicher sind. Ohne eine wirksame Regulierung wäre das Vertrauen der Anleger, insbesondere institutioneller Investoren, stark beeinträchtigt. Daher ist die Schaffung eines Gleichgewichts zwischen den beiden Interessen der Anonymität einerseits und der Sicherheit andererseits notwendig.

Dies dient dem Schutz der Allgemeinheit und dem Wohl aller Marktteilnehmer – also nicht nur dem Schutz der Verbraucher, sondern auch den Interessen der Kryptowerte-Emittenten und -Dienstleistern.

Zusammenfassend lässt sich festhalten, dass die Betroffenenrechte nach der DSGVO sowohl in der Kryptowertetransferverordnung als auch in der MiCA-Verordnung grundsätzlich gewahrt bleiben, wenn auch unter gewissen, klar definierten Einschränkungen, die erforderlich sind, um den rechtlichen und regulatorischen Anforderungen in einem zunehmend komplexen Marktumfeld gerecht zu werden. Es bleibt abzuwarten, wie insbesondere die MiCA-Verordnung in der Praxis umgesetzt wird und ob eine weitere Anpassung der datenschutzrechtlichen Rahmenbedingungen erforderlich sein wird.

Langfristig werden allerdings beide Verordnungen sicherlich zu einem höheren Maß an Transparenz, Verbraucherschutz und Marktsicherheit im gesamten Krypto-Sektor beitragen, ohne die Rechte der Betroffenen unverhältnismäßig stark einzuschränken.

8. Literaturverzeichnis

- Bergauer Christian, Jahnel Dietmar (Hrsg.) (2018). DSGVO und DSG. Das neue Datenschutzrecht. Wien: Jan Sramek Verlag
- BGBI. Nr. 69/2021. Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung - KryptoWTransferV), ausgegeben am 29. September 2021. Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/3-Verkuendete-Verordnung.pdf?__blob=publicationFile&v=4
(letzter Zugriff: 5.10.2023)
- Bitkom Bundesverband, Informationswirtschaft, Telekommunikation und Neue Medien e.V (2021). Bitkom Stellungnahme zum Arbeitsentwurf des Bundesfinanzministeriums für eine Kryptowertetransferverordnung (KryptoTransferV). Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-bitkom.pdf?__blob=publicationFile&v=2
(letzter Zugriff: 5.10.2023)
- Blockchain Bundesverband e.V. (2021). Kryptowertetransferverordnung. Stellungnahme des Blockchain Bundesverband e.V.. Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-blockchain.pdf?__blob=publicationFile&v=2
(letzter Zugriff: 5.10.2023)
- Brutkasten, Völkel, Oliver, MiCA: Was Krypto-Dienstleister jetzt wissen müssen, vom 14. Juni 2023, 26. März 2024. Abgerufen unter:
<https://brutkasten.com/artikel/mica-was-krypto-dienstleister-jetzt-wissen-muessen?ref=articletext>
(letzter Zugriff: 22.09.2024)
- Bundesministerium der Finanzen, Referat Digitale Kommunikation und Social Media (2021a). Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung – KryptoWTransferV). Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/0-Verordnung.html (letzter Zugriff: 5.10.2023)
- Bundesministerium der Finanzen (2021b). Arbeitsentwurf des Bundesministeriums der Finanzen. Kryptowertetransferverordnung (KryptoTransferV). Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/1-Referentenentwurf.pdf?__blob=publicationFile&v=3
(letzter Zugriff: 5.10.2023)

Bundesverband der Geldwäschebeauftragten e.V. (2021). Stellungnahme zum Referentenentwurf einer Verordnung des Bundesministeriums der Finanzen über verstärkte Sorgfaltspflicht bei der Übetragung von Kryptowerten (Kryptowertetransferverordnung – KryptoTransferV). Abgerufen unter: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-bvgb.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Deutsche Börse Group (2021). Stellungnahme der Gruppe Deutsche Börse zum Referentenentwurf der Kryptotransferverordnung. Abgerufen unter: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-gdb.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Die Deutsche Kreditwirtschaft (2021). Stellungnahme zum Arbeitsentwurf des Bundesministeriums der Finanzen für eine „Kryptowertetransferverordnung (KryptoTransferV)“. Abgerufen unter: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-dk.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Europäisches Parlament, Märkte für Kryptowerte, Legislative Entschließung des Europäischen Parlaments vom 20. April 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937 (COM(2020)0593 – C9-0306/2020 – 2020/0265(COD)), Abgerufen unter: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0117_DE.pdf. (letzter Zugriff: 18.09.2024)

Europäischer Wirtschafts- und Sozialausschuss (2021). Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowährungen und zur Änderung der Richtlinie (EU) 2019/1937 (COM(2020) 593 final — 2020/0265 (COD)) — 49 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Pilotregelung für auf der Distributed-Ledger-Technologie basierende Marktinfrastrukturen (COM(2020) 594 final — 2020/0267 (COD)). Abgerufen unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020AE4982&from=EN> (letzter Zugriff: 09.09.2024)

Europe Direct Info Point Europa Hamburg zu: Die neue europäische Krypto-Verordnung MiCA-VO. Abgerufen unter: <https://infopoint-europa.de/de/articles/mica-verordnung> (letzter Zugriff: 07.09.2024)

Finanzmarktaufsicht (2024). Stellungnahme zum Begutachtungsentwurf für ein Bundesgesetz, mit dem das Bundesgesetz über das Wirksamwerden der

Verordnung (EU) 2023/1114 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (MiCA-Verordnung-Vollzugsgesetz – MiCA-VVG) erlassen wird sowie das Finanzmarktaufsichtsbehördengesetz, das Bankwesengesetz, das HinweisgeberInnenschutzgesetz und das Alternative Investmentfonds Manager-Gesetz geändert werden

Abgerufen unter:

[file:///Users/anna/Downloads/FMA-LE0001.220_0003-INT_2024-1-](file:///Users/anna/Downloads/FMA-LE0001.220_0003-INT_2024-1-A_24.05.2024_.pdf)

[A_24.05.2024_.pdf](file:///Users/anna/Downloads/FMA-LE0001.220_0003-INT_2024-1-A_24.05.2024_.pdf)

(letzter Zugriff: 22.09.2024)

Futurum Bank AG (2021). Stellungnahme zur Kryptowertetransferverordnung.

Abgerufen unter:

https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-futurum.pdf?__blob=publicationFile&v=3

(letzter Zugriff: 5.10.2023)

G7-Arbeitsgruppe „Stablecoins“, Bericht „Untersuchung der Auswirkungen globaler Stablecoins“ („Investigating the impact of global stablecoins“), 2019, 26. März 2024. Abgerufen unter:

<https://www.bis.org/cpmi/publ/d187.pdf>

(letzter Zugriff: 15.09.2024)

Geldwäschegesetz – GwG. Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten. Abgerufen unter:

https://www.gesetze-im-internet.de/gwg_2017/GwG.pdf (letzter Zugriff: 4.2.2024)

Jahnel Dietmar, Pallwein-Prettner Angelika (2021). Datenschutzrecht. Wien: Facultas Verlags- und Buchhandels AG

Kapilendo AG (2021). Gemeinsame Stellungnahme von Kapilendo AG und Bloxxon AG zum Referentenentwurf für eine Rechtsverordnung des Bundesministeriums der Finanzen über verstärkte Sorgfaltspflicht bei der Übertragung von Kryptowerten (Kryptowertetransferverordnung). Abgerufen unter:

https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-kapilendo.pdf?__blob=publicationFile&v=2

(letzter Zugriff: 5.10.2023)

Khayat Philipp (2023). Kryptowerte und Kryptowährungen. Chancen und Risiken, Regulierungsinitiativen der Europäischen Union. Berlin: Gans Verlag

LSP, Lindemann, Schwennicke & Partner (2021). Stellungnahme zum

Referentenentwurf der KryptoTransferV. Abgerufen unter:

https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-lsp.pdf?__blob=publicationFile&v=2

(letzter Zugriff: 5.10.2023)

Pichler, Christina-Maria / Reiterer, Peter, Die MiCA-Verordnung – auf dem Weg zu einem fairen Kryptomarkt, Digitalisierung & IT, Compliance Praxis 2023, 38.

Reißler Ann-Kathrin (2022). EuGH erklärt EU-Geldwäscherichtlinie für teilweise ungültig. Abgerufen unter:
<https://asd-law.com/news/eugh-erklaert-eu-geldwaescherichtlinie-fuer-teilweise-unguelteig/> (letzter Zugriff: 27.4.2024)

Richter Andreas, Philipp Christoph, Viskorf Stephan, Haag Maximilian, Hemmen Katharina, Gollan Katharina (2022). EuGH erklärt EU-Geldwäscherichtlinie teilweise für rechtswidrig. Abgerufen unter:
<https://www.pe-magazin.de/eugh-erklaert-eu-geldwaescherichtlinie-teilweise-fuer-rechtswidrig/> (letzter Zugriff: 27.4.2024)

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Abgerufen unter:
<https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31995L0046>, (letzter Zugriff: 20.09.2024)

Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/E, ABl. L 173 vom 12.6.2014, S.349. Abgerufen unter:
<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014L0065&from=DE> (letzter Zugriff: 15.09.2024)

Transparency International Deutschland e.V., Arbeitsgruppe Finanzwesen (2021). Stellungnahme von Transparency International Deutschland e.V. zum Referentenentwurf über verstärkte Sorgfaltspflicht bei der Übertragung von Kryptowerten (Kryptowertetransferverordnung – KryptoTransferV). Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-transparency.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Verband der Auslandsbanken in Deutschland e.V. (2021). Stellungnahme des Verbands der Auslandsbanken in Deutschland e.V. (VAB) zum Entwurf einer Verordnung des Bundesministeriums der Finanzen (Ministerverordnung) über verstärkte Sorgfaltspflichten bei der Übertragung von Kryptowerten (Kryptowertetransferverordnung – KryptoTransferV) aufgrund des § 15 Absatz 10 Satz 1 Nummer 1 des Geldwäschegesetzes (GwG). Abgerufen unter:
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-vab.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006 (Text von Bedeutung für den

EWK). Abgerufen unter:

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015R0847>
(letzter Zugriff: 17.10.2023)

Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937. Abgerufen unter:

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1114>
(letzter Zugriff: 09.09.2024)

Wirtschaftsrat der CDU e.V. (2021). Stellungnahme zum Referentenentwurf des Bundesministeriums der Finanzen zu einer Kryptowertetransferverordnung. Abgerufen unter:

https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/Stellungnahme-wd.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 5.10.2023)

Abstract

Die MiCA-Verordnung und die Kryptowertetransferverordnung erfordern eine umfassende Datenerfassung und -verarbeitung, was zu einem Spannungsverhältnis mit dem Datenschutz führt. Dank Ausnahmeregelungen der DSGVO können die Betroffenenrechte eingeschränkt werden, um die Verordnungen effektiv durchzusetzen und die regulatorische Kontrolle des Krypto-Markts zu gewährleisten. Dies ist notwendig, um Sicherheitsrisiken zu minimieren. Beide Verordnungen schränken Rechte wie Transparenz, Löschung und Auskunft teilweise ein, um die Marktstabilität und das Vertrauen der Investoren zu sichern. Die Balance zwischen Anonymität und Sicherheit soll den Schutz aller Marktteilnehmer gewährleisten. Langfristig werden die Verordnungen mehr Transparenz, Verbraucherschutz und Marktsicherheit schaffen, ohne die Betroffenenrechte unverhältnismäßig einzuschränken.