Stellungnahme

Regierungsentwurf zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (GwG-Novelle)

09. September 2019

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Julian Grigo
Bereichsleiter Digital Banking & Financial Services
T +49 30 27576-126 | M +49 175 5848805 | @Bitkom_Finance

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Einleitung

Das Bundesministerium der Finanzen legte am 20. Mai 2019 den Referentenentwurf zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (Richtlinie [EU] 2018/843) in nationales Recht vor. Wir begrüßen die zeitige Umsetzung der Richtlinie und dass der Bundesgesetzgeber erkannt hat, dass es neben der Erfassung von Kryptowerten in der GwG-Novelle eine Notwendigkeit gibt, innovative und gleichzeitig sichere Identifizierungsverfahren zuzulassen, um den sich im Umbruch befindlichen und zunehmend dynamischen digitalen Finanzmarktplatz Deutschland nicht in seinem Wachstum zu behindern. Bereits im Laufe des bisherigen Gesetzgebungsprozesses wurden einige wichtige Änderungen im Vorschlag aufgenommen, die sich jetzt im Regierungsentwurf wiederfinden.

Jedoch sehen wir einigen Anpassungsbedarf, damit die nationale Umsetzung der Vierten Geldwäscherichtlinie in das deutsche Recht nicht zu Standortnachteilen führt und weiterhin innovative Geschäftsmodelle ermöglicht, ohne den Zweck der Geldwäscherichtlinie aus dem Blick zu verlieren. Hinsichtlich einiger der vorgeschlagenen Änderungen möchten wir nachfolgend einige Anmerkungen zum Regierungsentwurf einbringen.

Kernforderungen des Bitkom:

- In der Abweichung der deutschen Umsetzung von der EU-Richtlinie sehen wir die Gefährdung des einheitlichen Binnenmarktes. Viele unserer Finanzdienstleister agieren über nationale Grenzen hinweg in ganz Europa. Gerade für junge, stark wachsende FinTech-Unternehmen stellt jede Abweichung von der EU-Gesetzgebung eine Wachstumshürde dar und benachteiligt sie gegenüber ausländischen Wettbewerbern. Wir empfehlen

daher weitere Harmonisierungsbemühungen.

- Gerade bei KYC-Prozessen im Rahmen des Kunden-Onboarding besteht noch erhebliches Verbesserungspotential. Die Nachnutzung von Daten zur Identifizierung muss ermöglicht werden. Die Regelungen zum Verlassen auf Dritte müssen flexibler ausgestaltet werden, um digitale Lösungen nicht zu blockieren. Konkret beinhaltet der RegE Beschränkungen zum Rückgriff auf „verpflichtete Dritte“ gemäß § 17 Abs. 3 a GwG-E und stellt somit für innovative deutsche Zahlungs- und Identitätsdienstleister einen erheblichen kompetitiven Nachteil gegenüber EU- und außereuropäischen Wettbewerbern dar. Soweit ersichtlich bestehen in keinem anderen EU-Land derartig strikte Anforderungen.

- Wir empfehlen, dass bei Banken erhobene Identifizierungsdaten von Dritten genutzt werden dürfen, sofern entsprechende Erlaubnistatbestände greifen. Der bisherige Entwurf (§ 11 a RegE) fördert jedoch gemeinsam mit der nicht flächendeckend zur Verfügung stehenden Nutzung des eID sowie dem noch immer andauernden Diskurs um das für unsere Unternehmen unabdingbare VideoIdent-Verfahren sogenannte Lock-In-Effekte. Diese entstehen dadurch, dass der einfache Kontowechsel für Endkunden behindert wird. Schließlich bedeutet dies ein großes Hemmnis für das Wachstum innovativer Unternehmen.

- Es bedarf weiterer Klarstellung zu Details zur Kryptoverwahrlizenz. So ist unklar, weshalb Gesellschaften, die eine neue Kryptoverwahrlizenz beantragen, keine weitere Bank-, CCP-, oder CSD-Lizenz halten dürfen. Auch Details z.B. zur Timeline für Anträge, Anforderungen, Eigenkapital, Compliance, Audit, IT-Sicherheit etc. fehlen bisher und sollten aufgenommen werden. Wir halten es daher noch für bedenklich, in der aktuellen sehr dynamischen Entwicklungsphase in diesem Bereich einen nationalen Vorstoß zu wagen, der nicht auf EU-Ebene harmonisiert und international möglicherweise auch nicht konsensfähig ist.

- Das Transparenzregister muss dringend zukunftsfähig ausgestaltet und mit einer entsprechenden Schnittstelle versehen werden. Die Vorgabe des § 23a Abs. 2 GwG (RegE) erlaubt lediglich eine manuelle Erfassung von Meldungen an die registerführende Stelle über deren Website. Dies kann heutzutage nicht als moderne und digitale Erfassung bewertet werden. Wir empfehlen standardisierte elektronische Schnittstellenanbindungen. Darüber könnten dann bspw. Registrierungen abgewickelt werden sowie Datenabrufe nach § 11 Abs. 5 Satz 2 GwG (RegE) und Meldepflichten automatisiert werden.

Bitkom bedankt sich daher für die Gelegenheit zur Stellungnahme zum Entwurf und möchte im Folgenden auf die Details des Regierungsentwurfs wie folgt eingehen:

I. § 8 Absatz 4 Sätze 1 und 2 GwG-Entwurf

Die mit der Neufassung der Sätze 1 und 2 eingeführte Strukturierung lässt aus unserer Sicht Möglichkeit unterschiedlicher Interpretation zu. Während Satz 1 die Beachtung weiterer gesetzlicher Bestimmungen bei der Löschung von Aufzeichnungen festhält, wird in dem nachfolgenden Satz 2 eine Löschung „in jedem Fall" nach Ablauf von zehn Jahren festgesetzt. Durch die Reihenfolge sind Missverständnisse in der Auslegung möglich.

Wir würden daher eine Formulierung in Anlehnung an die aktuell gültige Fassung des Geldwäschegesetzes bevorzugen, daher unser Vorschlag:

„Die Aufzeichnungen und sonstige Belege nach den Absätzen 1 bis 3 sind fünf Jahre aufzubewahren und spätestens nach Ablauf von zehn Jahren zu vernichten, soweit nicht andere gesetzliche Bestimmungen über Aufzeichnungs- und Aufbewahrungspflichten eine längere Frist vorsehen."

II. § 8 Absatz 4 Sätze 3 und 4 GwG

Die Sätze 3 und 4 sind leider in dem Entwurf nicht angepasst worden, wodurch sich unterschiedliche Aufbewahrungsfristen ergeben.

1. Nach Satz 3 i.V.m § 10 Abs. 3 Satz 1 Nr. 1 beginnt die Löschfrist für die Erst-Dokumentation der allgemeinen Sorgfaltspflichten in Abhängigkeit vom Zeitpunkt der Beendigung der Geschäftsbeziehungen.

2. Nach Satz 4 beginnt die Löschfrist für alle übrigen Dokumentationen mit dem Datum der Feststellung der Angabe. Unter diese Dokumentationen dürften unter Berücksichtigung des § 10 Abs. 3a, Satz 2 GwG-Entwurf auch Dokumentationen zu laufenden Sorgfaltspflichten fallen (umgangssprachlich „Monitoring der Geschäftsbeziehung").

Durch diese unterschiedlichen Aufbewahrungsfristen, sehen wir die Gefahr das aktuellere Dokumentationen gelöscht werden müssen, wohingegen veraltete Erst-Dokumentationen weiterhin vorhanden sind. Im Rahmen der dauerhaften Nachvollziehbarkeit über signifikante Änderungen während des Geschäftsverhältnisses würden somit Lücken

entstehen. Wir würden daher an dieser Stelle eine Vereinheitlichung der Fristen begrüßen. Bereits die entsprechende EU-Richtlinie 2015/849 ist an dieser Stelle ungünstig. Entsprechend der Regelung in Artikel 40 Abs. 1 Satz 3 und 4 wäre über die Möglichkeit , eine weitere Aufbewahrung nach einer eingehenden Prüfung ihrer Erforderlichkeit und Verhältnismäßigkeit zu gestatten, wenn dies für die Verhinderung, Aufdeckung oder Ermittlung von Geldwäsche oder Terrorismusfinanzierung für erforderlich gehalten wird, ein angemessenes Vehikel, um diese Lücken zu schließen.

III. § 11a-Änderungen

Bitkom begrüßt ausdrücklich die Einführung der spezialgesetzlichen Ermächtigung in §11a RegE.

Aus datenschutzrechtlichen Gesichtspunkten wirft der § 11 a GwG-Neu Fragen auf. Die Regelung ist insoweit problematisch, als sie nicht klarstellt, dass jedenfalls ein Teil dieser Daten eben gerade nicht nur wegen des GwG erhoben wird. Kreditinstitute sind zB auch nach der AO verpflichtet, Angaben zu ihren Vertragspartnern (zu steuerrechtlichen) Zwecken zu verarbeiten. Darüber hinaus ist es auch nach dem HGB verpflichtet, Vertragspartner zu kennen und jedenfalls diese Daten festzuhalten. Schließlich werden Kundendaten wie der Name und die Anschrift auch zur Erfüllung der vertraglichen Pflichten des Kreditinstituts gegenüber seinen Kunden benötigt, weshalb sie von den Kunden auch zu diesem Zweck zur Verfügung gestellt werden. Hier muss unbedingt klargestellt werden, dass - soweit die Daten auch aus anderen Zwecken erhoben werden und verarbeitet werden dürfen - die hier aufgenommene Einschränkung nicht gilt, sondern die allgemeinen Regeln des Datenschutzes, die durchaus in gewissem Rahmen eine Zweckänderung erlauben. Ohne eine solche Klarstellung ist künftig möglicherweise streitig, ob ein Verpflichteter die Adresse seines Vertragspartners z. B. für Anschreiben zu Werbezwecken nutzen darf (was nach derzeitiger datenschutzrechtlicher Grundlage unstreitig der Fall ist, solange der Kunde nach Wettbewerbsrecht nicht widersprochen hat).

Aus wettbewerblichen Gesichtspunkten erscheint noch problematisch, dass der Wortlaut von § 11 a RegE einer Nutzung der bei Banken vorhandenen Identifizierungsdaten der Kunden z.B. zur Registrierung bei einem Vertrauensdiensteanbieter zwecks Erstellung eines qualifizierten Zertifikates entgegensteht. Dies stellt nach unserer Ansicht jedoch – solange das VideoIdent-Verfahren umstritten und auf Grundlage der Verfügung beschränkt bleibt und eID-Dienste noch nicht flächendeckend nutzbar sind – die derzeit einzige Möglichkeit dar, qualifizierte Signaturen massenfähig zu machen.

Folgegeschäftsmodelle müssen in jedem Fall weiterhin möglich bleiben. Die Bank/der Verpflichtete muss daher die personenbezogenen Daten aus der Identifizierung außerdem zum Zweck der Führung der Geschäftsbeziehung mit dem Kunden speichern/verarbeiten dürfen.

Der sich im Umbruch befindlichen und zunehmend dynamischen digitalen Finanzmarktplatz Deutschland darf nicht in seinem Wachstum behindert werden. Gerade bei KYC-Prozessen im Rahmen des Kunden-Onboarding besteht noch erhebliches Verbesserungspotential. Viele Kunden brechen langwierige und mit Medienbrüchen verbundene Identifizierungsverfahren erfolglos und frustriert ab. Dies führt nicht zu einer verbesserten Geldwäscheprävention, sondern einzig zu vermindertem Wettbewerb im Finanzdienstleistungssektor. Neue Anbieter und innovative Zahlungs- und Identitätsdienstleister werden durch die sich aus unnötig mühsamen Kontoeröffnungsprozessen ergebenden Lock-In Effekte benachteiligt. Wir befürchten, dass die in Deutschland regulierten und niedergelassenen Zahlungsinstitute durch die vorgeschlagenen Änderungen des GwG einen erheblichen kompetitiven Nachteil gegenüber EU- und außereuropäischen Wettbewerbern erleiden.

§ 11 a Absatz 1 RegE sollte daher hinsichtlich des Wortlauts z.B. wie folgt angepasst werden: „...eine Verarbeitung zu anderen Zwecken ist ohne eine andere Rechtsgrundlage nicht zulässig“. Jedenfalls die Einwilligung des Kunden muss hier stets möglich sein. Der Betroffene hat das Recht, selbst über die Nutzung seiner Daten zu entscheiden. Insoweit könnten auch eigene Interessen der Vertragspartner bestehen. Die DS-GVO stellt die Autonomie und Hoheit des Bürgers über seine Daten in den Mittelpunkt. Das Verbot des § 11 a Abs. 1 GwG-RegE würde bei wörtlicher Auslegung selbst solche Datenverarbeitungsvorgänge verbieten zu denen der Nutzer dem Verpflichteten eine wirksame separate Einwilligung erteilt hat. Dem Verpflichteten wäre es daher selbst dann untersagt, die in Erfüllung ihrer Sorgfaltspflichten erhobenen personenbezogenen Daten zu verarbeiten, wenn eine wirksame separate Einwilligung des Nutzers in die Datenverarbeitung vorliegt oder sich eine Rechtfertigung aus anderen von der DS-GVO anerkannten Zwecken ergibt, z.B. anderweitig berechtigtes oder vertragliches Interesse.

Es sollte zudem noch geprüft werden, inwieweit sich Services, die in der Übertragung der bereits erhobenen Daten zu Dritten bestehen mit dem Erbringen von vertraglichen Diensten bzw. dem Recht auf Datenportabilität aus Art. 20 DS-GVO in Verbindung stehen, um zu gewährleisten, dass durch den Kunden nachgefragte Dienste auch tatsächlich ausgeführt werden können (vgl. potentielle Einschränkungsmöglichkeiten in Art. 20 Absatz 3 DS-GVO).

IV. § 17 Abs. 3 a GwG-E Ausführung der Sorgfaltspflichten durch Dritte

Die Möglichkeit zur auch gesetzlich verankerten Möglichkeit zur Weitergabe und Wiederverwendung von Identifizierungsdatensätzen zur Erfüllung eigener Sorgfaltspflichten ist grundsätzlich begrüßenswert und entspricht der seit kurzem auch in den Auslegungs- und Anwendungshinweisen der BaFin verankerten aufsichtsbehördlichen Praxis. Insbesondere im Bereich der Identifikation des Kunden, z.B. bei Begründung einer Geschäftsbeziehung, kann die Vermeidung wiederholten Identifizierungsaufwandes zu einer erheblichen Wettbewerbsverbesserung durch einfachere Konteneröffnungen und damit -wechsel sowie zu erheblichen Kosteneinsparungen führen. Der „Lock-In-Effekt", der sich aus unnötig aufwändigen Kontoeröffnungsprozessen ergibt, kann erheblich reduziert werden. Um jedoch eine darauf zielende praktische Anwendung des § 17 Abs.3a GwG-E zu erreichen, sollte die gesetzlichen Voraussetzungen für die mehrfache Nutzung von Identifizierungsdatensätzen praxisgerechter ausgestaltet werden. Dies wird leider auch im vorliegenden Regierungsentwurf durch die aus den – bereits vielfach kritisch kommentierten – Auslegungs- und Anwendungshinweisen (AuAs) der BaFin nahezu inhaltsgleich ins Gesetz übernommenen Regelungen nicht erreicht.

Die klarstellenden Änderungen zum Territorialprinzip (S. 95 f. des Regierungsentwurfs) sind grundsätzlich nachvollziehbar und entsprechen der Umsetzungssystematik der 4. GW-RL.

Im Lichte der Geldwäsche-Richtlinie selbst, welche die Bedeutung auch der nationalen Schaffung innovativer Identifizierungsverfahren ausdrücklich anerkennt, ist jedoch eine Beschränkung der Wiederverwendung auf Datensätze, die durch „verpflichtete Dritte" nach Abs. 1-4 erhoben worden sind, zu eng gegriffen. Die auf Seite 95 f. des Regierungsentwurfs enthaltene Begründung, dass mit der Beschränkung auf „verpflichtete Dritte" verhindert werden soll, dass „Dienstleister Datenpools aufbauen, die *„keiner kontinuierlichen Überwachung (Monitoring) und den laufenden Überprüfungen einer „lebenden" Geschäftsverbindung unterliegen",* greift verfängt insoweit nicht, als es nur um den Tatbestand der Erstidentifizierung, quasi den „Erstkontakt" geht. Die kontinuierliche Überwachung obliegt grundsätzlich dem Verpflichteten, der auf den von dem Dritten (i.S.d. § 17 Abs. 5) erhobenen Datensatz zu Beginn der Geschäftsbeziehung zurückgreift. Von der Erstidentifizierung ist die kontinuierliche Überwachung und Aktualisierungspflicht zu unterscheiden. Gemäß § 17 Abs. 5 Satz 1 GwG können Verpflichtete die Durchführung der Maßnahmen, die zur Erfüllung der allgemeinen Sorgfaltspflichten gemäß § 10 Abs. 1 Nr. 1 bis 4 GwG erforderlich sind, [...] auf Dritte übertragen. Diese Aufzählung in § 17 Abs. 5 S. 1 ist abschließend. Das bedeutet, die

Durchführung der kontinuierlichen Überwachung und Aktualisierung nach § 10 Abs. 1 Nr. 5 GwG sowie erhöhter Sorgfaltspflichten durch Dritte und andere geeignete Personen und Unternehmen gemäß § 17 Abs. 5 GwG ist bereits gesetzlich nicht gestattet. Insoweit kann sie auch nicht als Begründung für einen notwendigen Ausschluss Dritter aus der „Wiederverendungsmöglichkeit“ herhalten.

In Ergänzung des bisherigen § 17 Absatz 5 Satz 2 wird zudem mit dem vorliegenden Regierungsentwurf die Anforderung aufgenommen, dass beim Rückgriff auf andere geeignete Personen und Unternehmen zur Erfüllung von Sorgfaltspflichten der Verpflichtete sicherzustellen hat, dass diese den Vorschriften des Geldwäschegesetzes entsprechen. Unabhängig davon, dass dies bereits zuvor über die Anforderungen des § 17 Abs. 5 GwG sicherzustellen war, bedeutet auch diese Klarstellung, dass auch die durch Dritte i.S.d. § 17 Abs. 5 GwG erhobenen Datensätze gemäß den Anforderungen des Geldwäschegesetztes und ggf. ergänzender aufsichtsbehördlicher Regelungen zu erfolgen hat.

Wir möchten in diesem Zusammenhang noch einmal die Sorge zum Ausdruck bringen, dass durch die neu eingefügten Beschränkungen zum Rückgriff auf „verpflichtete Dritte“ gemäß § 17 Abs. 3 a GwG-E, innovative deutsche Zahlungs- und Identitäts-Dienstleister einen erheblichen kompetitiven Nachteil gegenüber EU- und außereuropäischen Wettbewerbern erleiden werden. Soweit ersichtlich bestehen in keinem anderen EU-Land derartig strikte Anforderungen beim Rückgriff auf andere Verpflichtete zu Erfüllung der eigenen Sorgfaltspflichten. Zum Teil wird sogar in den aufsichtsbehördlichen Verfügungen die Wiederverwendung der durch einen dritten erhobenen Datensätze explizit aufgegriffen und genehmigt. Harmonisierung der Finanzindustrie ist jedoch aus unserer Sicht eine der Kernvoraussetzungen für den Digital Single Market und die Wettbewerbsfähigkeit der deutschen und europäischen Unternehmen. Gleiches gilt für die Harmonisierung von aufsichtsbehördlichen Entscheidungen, deren Bedeutung stetig zunimmt. Einige der europäischen Aufsichtsbehörden haben z.B. bereits erkannt, dass Praktikabilität der Anweisungen und Entscheidungen maßgeblicher Erfolgsfaktor der erfassten Unternehmen sein kann und so bei gleichzeitiger Wahrung der hohen Sicherheitsstandards die Wirtschaft gefördert wird. So heißt es etwa in der Wegleitung 2019/17 zu den i.S.v. Art. 14 Abs. 1 SPV anwendbaren Sicherungsmaßnahmen der Finanzmarktaufsicht Liechtenstein:

„Wird für die Identifikation des Vertragspartners ein externer Dienstleister verwendet, so kann dieser, sofern er die betreffende Person bereits für einen anderen Sorgfaltspflichtigen nach dem liechtensteinischen sorgfaltspflichtrechtlichen Vorgaben identifiziert hat, auf diese

Dokumentation zurückgreifen. Die Aktualität der vorhandenen Daten im Sinne des SPG und SPV ist in jedem Fall zu prüfen […].“

Der vorgeschlagene § 17 Abs. 3 a GwG geht aus den vorgenannten Gründen weit über die Regelung des Art. 25 der Änderungsrichtlinie zur 4. GW-RL hinaus.

Zur Vermeidung eines Standortnachteils für deutsche Unternehmen sollte es daher zulässig sein, dass auch solche Identifizierungsdatensätze erneut verwendet werden können, welche Dritte gesetzeskonform erhoben haben, welche nach Maßgabe des § 17 Abs. 5 GwG diese Daten für Verpflichtete zur Verfügung stellen. Hier wäre es begrüßenswert, wenn ein Dritter nicht Verpflichteter im Sinne des GwG sein muss, sondern es ausreichend ist, wenn er sich den entsprechenden Anforderungen beispielsweise an Kontrollmaßnahmen, die für einen Verpflichteten gelten, unterwirft. Auch hier kommt erneut die Bedeutung größerer Harmonisierung im EU-Raum zum Tragen. Es sollte angestrebt werden, die nationale Umsetzung der Richtlinie als Blueprint für die EU zu etablieren und so einen Standard für mehr Vereinheitlichung zu setzen.

Problematisch ist insbesondere die sehr kleinteilige Formulierung, die die aus den bereits vielfach kritisch kommentierten Auslegungs- und Anwendungshinweisen (AuAs) der BaFin bekannten Kriterien nahezu inhaltsgleich ins Gesetz übernimmt. Dies ist bereits Gesetzgebungssystematisch problematisch. Ein Gesetz hat andere Zwecke zu erfüllen als Auslegungs- und Anwendungshinweise einer Aufsichtsbehörde.

1. Wortlaut

„Der Dritte kann zur Identifizierung des Vertragspartners, einer gegebenenfalls für ihn auftretenden Person und eines wirtschaftlich Berechtigten auch auf eine anlässlich einer zu einem früheren Zeitpunkt erfolgten Identifizierung dieser Person eingeholte Informationen entsprechend Absatz 3 Satz 1 Nummer 2 zurückgreifen, sofern

1. die Identifizierung im Rahmen der Begründung einer eigenen Geschäftsbeziehung des Dritten und nicht unter Anwendung vereinfachter Sorgfaltspflichten erfolgt ist,

2. die Identifizierung oder die letzte Aktualisierung unter Einhaltung des § 12 vor nicht mehr als 24 Monaten abgeschlossen wurde,

3. für den Verpflichteten aufgrund äußerer Umstände keine Zweifel an der Richtigkeit der ihm übermittelten Informationen bestehen und

4. das Gültigkeitsdatum eines im Rahmen der Identifizierung oder der letzten Aktualisierung unter Einhaltung des § 12 gegebenenfalls verwendeten Identifikationsdokuments noch nicht abgelaufen ist.

Abs. 3 Satz 2 und 3 gilt entsprechend."

2. Gesetzesbegründung

„Die Einfügung von § 17 Abs. 3 a ermöglicht eine sinnvolle Vermeidung wiederholten Identifizierungsaufwandes bei ausreichender Wahrung des Grundgedankens des Geldwäschegesetzes, dass bei jeder Begründung einer Geschäftsbeziehung eine Identifizierung zu erfolgen hat.

Das GwG ermöglicht bereits unter den Voraussetzungen des § 11 Abs. 3 das Absehen von einer erneuten Identifizierung, sofern ein Kunde mehrfach Identifizierungspflichten bei ein und demselben Verpflichteten auslöst." (S. 95 des Regierungsentwurfs).

3. § 17 Abs. 3a Nr. 1

Das Verbot auf „unter Anwendung vereinfachter Sorgfaltspflichten" erhobene Identifizierungen zurückzugreifen scheint unter Risikogesichtspunkten nicht gerechtfertigt. Jedenfalls soweit der Verpflichtete selbst nur vereinfachte Sorgfaltspflichten zu erfüllen hat, sollte er auch auf im Rahmen vereinfachter Sorgfaltspflichten erhobene Identitäten eines Dritten zurückgreifen können.

Auch beim Rückgriff nach § 17 Abs. 3 a GwG-E bleibt der Verpflichtete für die Identifizierung verantwortlich. Insofern obliegt es dem Verpflichteten nachzuweisen, dass der ursprüngliche Identifizierungsprozess beim „Dritten" ausreichend war, um die eigenen auf Grundlage der Risikomatrix erstellten Vorgaben des Verpflichteten für eine Identifizierung zu erfüllen.

Empfehlung:

Der letzte Halbsatz des § 17 Abs. 3 a Nr. 1 „und nicht unter Anwendung vereinfachter Sorgfaltspflichten" sollte daher gestrichen werden.

„[...] sofern

1. die Identifizierung im Rahmen der Begründung einer eigenen Geschäftsbeziehung des Dritten ~~und nicht unter Anwendung vereinfachter Sorgfaltspflichten~~ erfolgt ist,“

4. § 17 Abs. 3a Nr. 2

Der 24 Monatszeitraum wurde bereits während den Anhörungen zu den AuAs kontrovers diskutiert. Es ist weiterhin kein Maßstab oder eine durchgreifende Erklärung ersichtlich, warum im Rahmen einer „lebenden“ Geschäftsbeziehung eines Instituts mit seinem Kunden 24 Monate als sicherer Zeitraum gelten sollen, 36, 48 oder 60 Monate jedoch nicht. Die durchgehenden Überwachungserfordernisse gegenüber seinen Kunden und den jeweiligen Zahlungsströmen, die ein reguliertes Institut zu erfüllen hat, ergeben über die Zeit ein sehr viel konkreteres Bild über die Identität eines Kunden als eine Erstidentifizierung.

Eine Gesetzesnovelle hat andere Zwecke zu erfüllen als die Auslegungs- und Anwendungshinweise (AuAs) der BaFin. Während bei den AuAs eine konkrete Nennung von Details und Zeiträumen, wie z.B. dem Monatszeitraum aus § 17 Abs. 3 a Nr. 2 GwG-E hilfreich ist und den regulierten Instituten Leitplanken in der praktischen Anwendung des Gesetzes vorgibt, birgt eine derartig strikte Festlegung von Zeiträumen im Rahmen eines abstrakten Gesetzes das große Risiko, dass auf Veränderungen im Marktumfeld, z.B. durch technologische Innovationen und anderweitige Disruptionen nicht ausreichend schnell reagiert werden kann.

Im Referentenentwurf nahm § 17 Abs. 3a Nr. 2 für die Auslösung der 24-Monatsfrist ausschließlich Bezug auf den Abschluss der (Erst-)Identifizierung. Insofern ist die Ergänzung um „die letzte Aktualisierung“ positiv zu bewerten. Zudem kann der Ergänzung entnommen werden, dass auch der Gesetzgeber erkannt hat, dass eine erst kürzlich GwG-konform aktualisierte Identität, die ursprünglich bspw. vor 36 Monaten erhoben wurde, deutlich aktueller und in Geldwäschehinsicht sicherer ist als eine vor 23 Monat erstmalig erhobene Identität. Dass diese Aktualisierung nach dem Regierungsentwurf allerdings „unter Einhaltung des § 12“ erfolgt sein muss, wirft Fragen auf. Ein uneingeschränkter Verweis auf die Anforderungen nach § 12 würde dazu führen, dass für eine Aktualisierung ggf. eine erneute vollständige Identitätsprüfung durchzuführen wäre. Gerade in einer laufenden Geschäftsbeziehung ist dies jedoch nicht nachvollziehbar. Vielmehr sollte bei einer bereits erfolgten GwG-konformen Identifizierung eine GwG-konforme Aktualisierung unter erleichterten Bedingungen auf Grundlage einer Risikoabwägung möglich sein. Dadurch soll die Möglichkeit der Weitergabe insbesondere nicht über das

aus Gesichtspunkten der Verhinderung der Geldwäsche und Terrorismusfinanzierung erforderliche Maß hinaus eingeschränkt werden.

Empfehlung:

Variante 1:

§ 17 Abs. 3 a Nr. 2 GwG-E ist ersatzlos zu streichen. Die AuAs der BaFin erscheinen hier ausreichend und bieten bei notwendigen Anpassungen ausreichend Flexibilität.

~~„sofern, […]~~

~~2. die Identifizierung oder die letzte Aktualisierung unter Einhaltung des § 12 vor nicht mehr als 24 Monaten abgeschlossen wurde,~~

Variante 2:

Soweit der Gesetzgeber zur Aktualität von Identifizierungsdaten eine Aussage treffen will, zeigen Erfahrungen mit anderen Legislativakten, dass eine abstraktere Formulierung vorzugswürdig ist. Der Aufsichtsbehörde, hier der BaFin, bliebe es insofern immer noch unbenommen bestimmte Zeiträume oder Aktualitätsperioden festzulegen. Insofern sollte § 17 Abs. 3 a Nr. 2 GwG-E wie folgt ergänzt werden:

„sofern, […]

2. der Identifizierungsdatensatz noch aktuell ist“.

Variante 3:

Soweit auch diese Anpassung dem Gesetzgeber nicht ausreicht, sollte § 17 Abs. 3 a Nr. 2 GwG-E für den Fall der Bezugnahme auf die letzte GwG-konforme Aktualisierung eine abstrakte Formulierung enthalten. Der Aufsichtsbehörde, hier der BaFin, bliebe insofern auch hier die Möglichkeit, bestimmte Parameter für die Aktualisierung festzulegen.

In diesem Fall wäre § 17 Abs. 3 a Nr. 2 GwG-E wie folgt anzupassen:

„sofern, […]

2. die Identifizierung oder die letzte Aktualisierung unter Einhaltung des § 12 vor nicht mehr als 24 Monaten ~~abgeschlossen~~ durchgeführt wurde,“

Variante 4:

Soweit auch diese Anpassung dem Gesetzgeber nicht ausreicht, sollte zumindest in der Gesetzesbegründung oder durch Auslegungshinweise der BaFin zu § 17 Abs. 3 a Nr. 2 GwG-E klargestellt werden, welche Anforderungen an eine GwG-konforme Aktualisierung gestellt werden. Eine GwG-konforme Aktualisierung müsste risikoadäquat erfolgen. Regelmäßig dürften die Anforderungen an eine Aktualisierung der Kundendaten im Rahmen einer bestehenden Geschäftsbeziehung daher einen geringeren Umfang haben, als die Anforderungen an eine GwG-konforme Erstidentifizierung. In diesem Fall wäre § 17 Abs. 3 a Nr. 2 GwG-E nicht anzupassen, sondern nur die Gesetzesbegründung bzw. die Auslegungshinweise der BaFin. Unter Bezugnahme auf das oben Gesagte sollte zudem ein anderer Zeitrahmen z.B. von 36 oder 60 Monaten diskutiert werden.

V. § 17 (Nummer 15 Doppelbuchstabe aa Begründungstext ab Seite 94)

Künftig sollen bei der Identifizierung von im Ausland ansässigen Personen durch Dritte, die im jeweiligen Ausland anerkannten Verfahren zulässig sein. Andernfalls würde die Identifikation von im Ausland ansässigen Personen maximal erschwert und deutschen Instituten ein erheblicher Wettbewerbsnachteil auferlegt. Der GwG-Regierungsentwurf greift diese Thematik auch bereits auf.

§ 17 GwG-RegE wurde im Vergleich zum Referentenentwurf auch dahingehend konkretisiert, dass bei der Identifizierung „von im Inland ansässigen Personen“ stets das deutsche GwG Anwendung finden muss.

Im Umkehrschluss bestünde somit bei der grenzüberschreitenden Dienstleistungserbringung weiterhin die Möglichkeit im Ausland ansässige Personen durch den Einsatz von (per se zuverlässigen) Dritten nach ausländischem Recht bzw. nach im Ausland anerkannten Verfahren zu identifizieren. Gemäß Gesetzesbegründung wird diese Möglichkeit jedoch dadurch eingeschränkt, dass man nicht auf irgendein Identifizierungsverfahren zurückgreifen darf, sondern dies den gleichen Sicherheitsstandards wie nach dem deutschen GwG zulässigen Verfahren entsprechen muss.

Aus unserer Sicht müssen die in den jeweiligen europäischen Mitgliedstaaten von der entsprechenden Aufsicht zugelassenen Identifizierungsverfahren auch weiterhin zulässig sein. Dies gilt insbesondere, da Institute mit den in Deutschland anerkannten Verfahren (hier insbesondere dem Videoidentifizierungsverfahren) bspw. aufgrund von Sprachbarrieren naturgemäß im grenzüberschreitenden Geschäft an Grenzen stoßen und eine Identifikation von im Ausland ansässigen Personen maximal erschwert würde.

Aus Bitkom-Sicht ist es daher erforderlich, dass auch Ausführungen in der Gesetzesbegründung zu § 17 (Nummer 15 Doppelbuchstabe aa ab Seite 94) klarer formuliert werden.

Dort heißt es aktuell:

„Der neue Wortlaut des Absatz 3 Satz 1 Nummer 1 und die Beschränkung auf Identifizierung von im Inland ansässigen Personen bedeutet nicht, dass der Verpflichtete nach dem Geldwäschegesetz beim Zurückgreifen auf Dritte nach Absatz 1 bei Identifizierungen in Auslandssachverhalten hinsichtlich der einzuhaltenden Standards völlig frei ist. Vielmehr gelten insoweit die dort die nach Absatz 1 Satz 2 vorausgesetzten Regulierungs- und Aufsichtsstandards, und nach Absatz 1 Satz 3 zusätzlich die Maßgabe, dass die Verantwortung für die Erfüllung der allgemeinen Sorgfaltspflichten beim Verpflichteten nach dem Geldwäschegesetz bleibt. Dieser Verantwortung für die Erfüllung von Sorgfaltspflichten wird ein Verpflichteter nach dem Geldwäschegesetze nicht gerecht, wenn er beispielsweise über die Einschaltung von Dritten nach Absatz 1 Satz 1 Verfahren für Identifizierungen nutzt, die nicht gleiche Sicherheitsstandards wie die sonstigen nach diesem Gesetz zulässigen Identifizierungsverfahren erfüllen."

Aus unserer Sicht sollte der letzte Satz in etwa wie folgt lauten:

„Dieser Verantwortung für die Erfüllung von Sorgfaltspflichten wird ein Verpflichteter nach dem Geldwäschegesetze nicht gerecht, wenn er beispielsweise über die Einschaltung von Dritten nach Absatz 1 Satz 1 Verfahren für Identifizierungen nutzt, die nicht die gleichen Sicherheitsstandards wie die im jeweiligen Zielland zulässigen Identifizierungsverfahren erfüllen. Dies gilt nur, wenn es sich bei dem Zielland um einen Mitgliedstaat handelt. Handelt es sich bei dem Zielland hingegen um ein Drittland, kann nicht auf die in diesem Land zulässigen Identifizierungsverfahren zurückgegriffen werden."

VI. Gesetzesbegründung zu § 17 Abs. 3 a mit Verbot der „Kettenweitergabe“ du § 17 Absatz 5

Der Gesetzgeber übernimmt die Maßgabe der BaFin aus den AuAs, dass ein Rückgriff auf einen Dritten zu Erfüllung eigener Sorgfaltspflichten nur auf solche Dritte zulässig ist, die die Erstidentifizierung des Kunden durchgeführt haben. Begründet wird dies mit einer Vermeidung der „Fehlerpotenzierung“ (S. 96 des Regierungsentwurfs).

Das vermeintliche Risiko einer „Fehlerpotenzierung“ wird nicht weiter belegt. Es ist daher unverständlich, dass „eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann“ und eine „Kettenweitergabe“ von Informationen nicht gestattet wird.

Regulierte Institute stellen eine der Säulen der Geldwäsche- und Terrorismusbekämpfung dar. Zwar bedarf es im aktuellen Überwachungssystem durchaus auch der Überwachung durch eine Aufsichtsbehörde. Die verpflichteten Institute, mit ihren Anti-Geldwäschebeauftragten und geschulten Mitarbeitern, sind jedoch ein wesentlicher Teil des Systems zur Verhinderung der Geldwäsche und Terrorismusfinanzierung.

Zitat, S. 96 des Regierungsentwurfs

„Die Voraussetzung des § 17 Absatz 3a Satz 1 Nummer 1, dass die Erhebung der Daten bzw. Informationen zur Erfüllung eigener Kundensorgfaltspflichten erfolgt sein muss beinhaltet schließlich, dass eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann – eine „Kettenweitergabe“ von Informationen ist somit nicht gestattet. Damit wird einer möglichen Fehlerpotenzierung entgegengewirkt.“

Die logische Verknüpfung von “Erhebung im eigenen Interesse“ und zwingender „Erstidentifizierung“ erschließt sich nicht. Wie bereits oben ausgeführt, bleibt der Verpflichtete auch bei Rückgriff auf einen Dritten für die Erfüllung seiner eigenen Sorgfaltspflichten, hier bei der Kundenidentifizierung, verantwortlich und erhebt auch diese Identität im „eigenen Interesse“ im Sinne des § 17 Abs. 1 und Abs. 3 a GwG.

Im Rahmen der Kundenidentifizierung regen wir zudem klarere Guidance an, wann bei der Überprüfung der Einhaltung der 10.000 Schwelle bei Bargeldtransaktionen eine Transaktion in zeitlicher Hinsicht als zusammenhängend betrachtet werden kann, wenn z.B. ein Kunde an Tag 1 etwas für 7.000 EUR bestimmte Produkte kauft und beispielsweise

zwei Tage später ähnliche Produkte für 4.000 EUR kauft. Hinweise darauf, wann identifiziert und dokumentiert werden muss oder ob die Pflicht nur bei zwei entsprechenden Zahlungen am gleichen Tag gilt, würde die praktische Umsetzung erleichtern.

Hinsichtlich der zur Identifizierung Verpflichteten, beinhaltet die „Erhebung der Daten bzw. Informationen zur Erfüllung eigener Kundensorgfaltspflichten“ aus unserer Sicht nicht, dass eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann. Zudem kann das dem Hinweis auf „Fehlerpotenzierung“ implizite Argument, dass eine durch einen anderen Verpflichten erhobene Identität vom nächsten Verpflichteten nicht mehr so genau oder sorgsam überprüft wird, wie eine erstmalig selbst erhobene Identität, nicht gelten gelassen werden. Auch hier gilt, vier Augen sehen mehr als zwei.

Vielmehr dürfte beim Rückgriff auf Dritte gemäß § 17 Abs. 1 GwG sogar eine Risikominimierung die Folge sein, da ein Verpflichteter, der auf die Identifizierung eines anderen verpflichteten „Dritten“ zurückgreift, diesen unmittelbar informieren würde, wenn er einen Fehler oder gar Anzeichen für Betrug bei der zuvor durch den Dritten erfolgten Identifizierung feststellt.

Soweit beide Institute denselben Kunden unabhängig voneinander, z.B. auf Grundlage eines gefälschten Ausweisdokuments, oder einer von beiden versehentlich falsch identifizieren, wäre eine Information des jeweils anderen Instituts unwahrscheinlich, da schlicht das Wissen über die anderweitig bestehende Geschäftsbeziehung fehlt.

Letztlich sollte erwähnt werden, dass bereits jetzt und auch zukünftig bestimmte Drei-Parteien-Verhältnisse bei der Identitätsdatenweitergabe nach dem GwG zulässig sind. Dies ist immer dann der Fall, wenn die Erstidentifizierung durch eine vertragliche Auslagerung gemäß § 17 Abs. 5 GwG an einen nicht GwG-Verpflichteten Dritten, z.B. einen Videoidentifikationsdienstleister, erfolgt, der die Erstidentifikation für ein reguliertes Institut (Bank 1) durchführt.

Soweit ein anderes verpflichtetes Institut (Bank 2) später auf diese Erstidentifikation zugreift, haben wir bereits einen Identitätsdatenweitergabe im Drei-Parteienverhältnis: Videoidentifikationsdienstleister – Bank 1 – Bank 2.

Konsequent weitergedacht, bedeutet dies, wenn ein verpflichtetes Institut (Bank 1) einen anderen Verpflichteten (Bank 2) vertraglich, d.h. auf Grundlage des § 17 Abs. 5 GwG, mit

der Identifizierung eines Kunden für Bank 1 beauftragen würde, anstatt auf Grundlage des § 17 Abs. 1 GwG auf Bank 2 zurückzugreifen, diese Bank 1 den Datensatz später sehr wohl an einen weiteren Verpflichteten (Bank 3) weitergeben könnte. Insofern erscheint das Verbot der Kettenweitergabe zwischen GwG-Verpflichteten auf Grundlage des § 17 Abs. 1 GwG systemwidrig.

Daraus sollte der Bundesgesetzgeber den Schluss ziehen, dass auch die Identitätsdatenweitergabe zwischen Verpflichteten im Drei-Parteienverhältnis: Bank 1 - Bank 2 – Bank 3 möglich sein sollte, also dann wenn der Erstidentifizierer eine Bank oder ein anderes reguliertes Institut war, welches die Erstidentifizierung im eigenen Interesse durchgeführt hat. Zumindest testweise sollte der Bundesgesetzgeber in Absprache mit der BaFin diese dreigliedrige Kettenweitergabe zulassen. Auf Grundlage des zuvor Gesagten ist wahrscheinlich, dass sich das Risiko der „Fehlerpotenzierung“ nicht realisiert, sondern vielmehr eine Risikominimierung eintritt.

Empfehlung:

Die folgende Passage aus der Gesetzesbegründung, S. 96, sollte gestrichen werden.

„Die Voraussetzung des § 17 Absatz 3a Satz 1 Nummer 1, dass die Erhebung der Daten bzw. Informationen zur Erfüllung eigener Kundensorgfaltspflichten erfolgt sein muss beinhaltet schließlich, dass eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann – eine „Kettenweitergabe“ von Informationen ist somit nicht gestattet. Damit wird einer möglichen Fehlerpotenzierung entgegengewirkt.“

Alternativ wäre folgende Formulierung denkbar:

„Die Voraussetzung des § 17 Absatz 3a Satz 1 Nummer 1, dass die Erhebung der Daten bzw. Informationen zur Erfüllung eigener Kundensorgfaltspflichten erfolgt sein muss, beinhaltet schließlich nicht, dass eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann – und schließt daher eine „Kettenweitergabe“ von Informationen ~~ist somit nicht gestattet~~ nicht aus. Die Verpflichteten haben für den Fall der mehrstufigen Weitergabe jedoch adäquate Sicherungsmaßnahmen zu treffen, damit dem Risiko einer möglichen Fehlerpotenzierung entgegengewirkt wird.“

Ebenso ist anzumerken, dass in § 17 Absatz 5 durch die Einfügung des Halbsatzes „...und der Verpflichtete hat sicherzustellen, dass die anderen geeigneten Personen und Unternehmen den Vorschriften dieses Gesetzes entsprechen“ eine neue Bewertung des vertraglichen Einsatzes „...andere geeignete Personen und Unternehmen“ vorgenommen wird. Hier sollte klargestellt werden, dass diese „anderen geeigneten Personen und Unternehmen“ nicht ausschließlich Verpflichtete sein können.

VII. Schnittstellenanbindung an das Transparenzregister, § 11 Abs. 5 Satz 2 und § 23 a Abs. 2 GwG (RegE)

Durch die 5. GW-RL müssen die Verpflichteten zusätzlich zu ihren sonstigen Pflichten sicherstellen, dass ihre Vertragspartner ihren Pflichten aus §§ 20, 21 GwG (RegE) nachgekommen sind und darüber hinaus mögliche Unstimmigkeiten an das Transparenzregister melden. Gleichzeitig stellt das Transparenzregister keine moderne Schnittstelle zur Verfügung, um diese Aufgaben (also den Abruf der Daten und die Rückmeldung von Unstimmigkeiten) zu erfüllen.

Es bedarf umfassender Nachbesserung, damit das Ziel des § 23a Abs. 2 GwG (RegE), „eine effiziente und digitale Erstattung von Unstimmigkeitsmeldungen“ zu ermöglichen (siehe S. 103 der Begründung).

Die Vorgabe des § 23a Abs. 2 GwG (RegE) ist weder ausreichend noch hilfreich – sie erlaubt lediglich eine manuelle Erfassung der Unstimmigkeitsmeldung an die registerführende Stelle über deren Website. Die manuelle Erfassung von Daten auf einer Website kann heutzutage nicht als moderne und digitale Erfassung nicht bewertet werden.

Hier sehen wir den Gesetzgeber in der Pflicht, allgemein (d.h. über § 23a GwG (RegE) hinausgehend) einen Betrieb des Transparenzregisters sicherzustellen, der modernen Anforderungen genügt, indem er standardisierte elektronische Schnittstellenanbindungen vorsieht. Darüber könnten dann bspw. Registrierungen abgewickelt werden sowie Datenabrufe nach § 11 Abs. 5 Satz 2 GwG (RegE) und Meldepflichten automatisiert werden. Auch für diese Vorgänge sieht die vorliegende Transparenzregisterdatenübermittlungsverordnung hierfür heute lediglich manuelle Erfassungen auf www.transparenzregister.de vor.

Die Aufforderung, elektronische Schnittstellen zum Transparenzregister anzubieten, berührt grundsätzliche Fragen zum Zugang bzw. zur Öffentlichkeit des Registers nicht. Sie zielt ausschließlich darauf ab, im Rahmen der bestehenden bzw. vorgesehenen

gesetzlichen Vorgaben für diejenigen zeitgemäße digitale und effiziente Lösungen zu schaffen, denen der Gesetzgeber Pflichten im Zusammenhang mit dem Transparenzregister auferlegt. Die im GwG bereits vorgesehenen Verordnungsermächtigungen müssen dazu genutzt werden, die Transparenzregisterdatenübermittlungsverordnung auf einen zeitgemäßen Stand zu bringen und damit zeitgemäße digitale Prozesse zu unterstützen.

VIII. § 56 GWG – Schuldhaftes Handeln

Bitkom begrüßt, dass die in § 56 des Referentenentwurfs zum GWG noch vorgesehen Verschärfung bei der Definition schuldhaften Handelns (Beurteilung, ob ein schuldhaftes Handeln vorliegt, sollte sich nur noch danach bestimmen, ob das Handeln vorsätzlich oder fahrlässig erfolgte) bereits angepasst wurde. Schuldhaftes Handeln ist in der jetzigen Fassung richtigerweise im § 56 GwG (RegE) wie bisher auch mindestens an die grobe Fahrlässigkeit (Leichtfertigkeit) geknüpft. An dieser Entwicklung sollte auch im weiteren Verhandlungsverlauf festgehalten werden.

IX. Kryptowerte

1. Definition und Ausgestaltung

Der RegE definiert Kryptowerte wie folgt:

„Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann“

Die Definition ist damit sehr weitgehend (§ 1 Abs. 11 S. 3 RegE-KWG, Seite 39), daher können Dienstleistungen für Kryptowerte ggf. gleichzeitig auch bestehende Bankgeschäfte bzw. CCP-/CSD-Geschäfte umfassen. Beispielsweise würden die Verwahrung von ausländischen, dematerialisierten Wertpapieren (die nach unserem Verständnis auch „digitale Darstellungen eines Wertes“ sind) damit unter die Definition der „Kryptowerte“ fallen.

Gleichzeitig fallen diese ausländischen, dematerialisierten Wertpapiere aber auch unter den Wertpapierbegriff des Depotgesetzes, welches daher für das Verwahrgeschäft vorrangig ist. Wichtig und richtig ist daher aus unserer Sicht die Erläuterung auf S. 125 des Regierungsentwurfs: Soweit Kryptowerte unter den Wertpapierbegriff des Depotgesetzes fallen, ist die Verwahrung Depotgeschäft im Sinne des § 1 Absatz 1 Satz 2 Nummer 5; § 1 Absatz 1 a Satz 2 Nummer 6 tritt dahinter zurück.

Eventuelle Überschneidungen mit anderen Regulierungsbereichen sollten insgesamt sorgfältig abgewogen werden, wenn wie hier der Geltungsbereich des GWG auf den Anlagebereich und damit auch auf das Wertpapiergeschäft und Depotgeschäft erweitert. Auch wenn es grundsätzlich zu begrüßen ist, dass in diesen Marktsegmenten durch eine klare Regulierung Rechtssicherheit geschaffen wird, halten wir es für problematisch, in der aktuellen sehr dynamischen Entwicklungsphase in diesem Bereich einen nationalen Vorstoß zu wagen, der nicht auf EU-Ebene harmonisiert und international möglicherweise auch nicht konsensfähig ist. Es kommt hinzu, dass der proprietäre und international noch nicht gefestigte Begriff „Kryptoverwahrgeschäft" nicht trennscharf im Hinblick auf andere digitale Finanzdienstleistungsgeschäfte definiert ist. Dies dürfte in der Praxis zu erheblichem Diskussionsbedarf führen, welche Dienstleistungen genau hierunter zu fassen sind. Dies könnte die Entfaltung des Binnenmarkts für innovative digitale Finanzdienstleistungen erheblich behindern (weitere Ausführungen hierzu unter Punkt 2-3).

Auch sollte eine Umsetzung möglichst nah an der Richtlinie erfolgen, um größtmögliche Harmonisierung sicherzustellen. Die Unterschiede zwischen EU-Richtlinie und der nun vorgeschlagenen nationalen Umsetzung stellen sich im Detail wie folgt dar:

EU-Richtlinie	RegE GWG-neu
„**virtuelle Währungen**" eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und **nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist** und die nicht den	**Kryptowerte im Sinne dieses Gesetzes** sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel

gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann;	akzeptiert wird **oder Anlagezwecken dient** und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann. **Keine Kryptowerte im Sinne dieses Gesetzes sind** **1. E-Geld im Sinne des § 1 Absatz 2 Satz 3 des Zahlungsdiensteaufsichtsgesetzes oder** **2. ein monetärer Wert, der die Anforderungen des § 2 Absatz 1 Nummer 10 des Zahlungsdiensteaufsichtsgesetzes erfüllt oder nur für Zahlungsvorgänge nach § 2 Absatz 1 Nummer 11 des Zahlungsdiensteaufsichtsgesetzes eingesetzt wird**.
„Anbieter von elektronischen Geldbörsen“ einen Anbieter, der Dienste zur Sicherung privater kryptografischer Schlüssel im Namen seiner Kunden anbietet, um virtuelle Währungen zu halten, zu speichern und zu übertragen.“	**die Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern oder zu übertragen, für andere (Kryptoverwahrgeschäft),“.**

Bitkom schlägt daher vor, im Hinblick auf den noch nicht abgeschlossenen internationalen Diskurs (siehe beispielsweise die G20-Erklärung von Fukuoka vom Juni 2019 zu Krypto-Assets) den Fokus im GWG-neu auf virtuellen Währungen bzw. die anwendungsneutralen Aspekte von Kryptowerten zu fokussieren und die anwendungsspezifischen Aspekte in dem für die jeweiligen Anwendungsbereiche relevanten Gesetzeskontexten zu regeln.

Unter GWG-Aspekten ist es u.E. wichtig sicherzustellen, dass ermittelt werden kann, wer die natürliche Person ist, die die Kontrolle über den kryptografischen Schlüssel ausübt. Dies umfasst zwei Aspekte:

- Sichere Identifizierung der handelnden Personen
- Sichere Generierung, Speicherung, Nutzung und Löschung der dieser Person zugeordneten kryptografischen Schlüssel (Vermeidung von Missbrauch des Schlüssels durch unberechtigte Dritte)

Darüber hinaus können beliebige Objekt, die einen wirtschaftlichen oder ideellen Wert verkörpern, durch einen kryptografischen Schlüssel repräsentiert werden (Tokenisierung).

Wenn diese Objekte einen Wert verkörpern, der gemäß der Definitionen in § 1 KWG als Finanzdienstleistung kategorisiert wird, dann könnte dieser Wert allgemein als „Kryptowert“ bezeichnet werden. Die Verwahrung (inklusive zuverlässiger Zuordnung von Wertobjekt zu kryptografischem Schlüssel, Verarbeitung und Transfer) dieser Krypto sollte allerdings bis auf weiteres unter die für die jeweilige Finanzdienstleistung gültigen gesetzlichen Bestimmungen fallen. Wenn der Markt für Kryptowerte sich stabilisiert und es sich herausstellen sollte, dass sich neue Rollen am Markt etablieren, die einer gesonderten Zulassung bedürfen, dann könnten diese Dienstleister als neue Finanzdienstleister in das KWG explizit aufgenommen werden. Dies sollte jedoch nur dann erfolgen, wenn die Rolle dieser neuen Finanzdienstleister zumindest EU-weit einheitlich definiert und reguliert wird (Beispiel Zahlungsdienstleister und PSD2).

Hierbei ist stets auch die Unterscheidung zwischen digitalen Werten versus Kryptowerten einzubeziehen:

- Der Inhaber des kryptografischen Schlüssels ist Eigentümer und Besitzer der mit diesem Schlüssel verbundenen Werte, und zwar so, dass diese Werte vom Eigentümer – je nach Konstellation mit oder ohne Einschaltung von Intermediären - weiter an einen neuen Eigentümer transferiert werden können. Die Werte befinden sich unter seiner alleinigen Kontrolle. Die Blockchain oder DLT stellt lediglich die Infrastruktur bereit (DLT = Autobahn, Kryptowert = Auto)

- Unterschied zu digitalen Werten: Digitale Werte werden i.d.R. von einem Dritten verwaltet, der damit der Besitzer der digitalen Werte ist (nicht der Eigentümer). Die Ausführung einer Transaktion bedarf immer eines Intermediärs (zum Beispiel Giralgeld).

- Der wesentliche Unterschied liegt somit in der Kontrolle, die der Eigentümer mittels seines privaten Schlüssels ausüben kann. Darum sollte sich eine dedizierte Regulierung von Kryptowerten auf diesen Aspekt fokussieren.

Im internationalen und EU-Vergleich könnte der zukünftige deutsche Kryptomarkt durch den vorliegenden RegE daher im Ergebnis zu eng reguliert werden. Es sollten Festlegungen vermieden werden, die einer späteren EU-Regulierung zuwiderlaufen könnten. Das Kryptoverwahrgeschäft sollte möglichst in Anlehnung an bisherige Gesetzgebung gestaltet sein (z.B. Anwendung einer CSDR für Security-Token).

2. Handelbarkeit von Security Tokens

Die Abwicklung, Verwahrung und Verwaltung von Kryptowerten im bestehenden Depot-System, einschließlich des Clearings und des Settlements durch Zentrale Kontrahenten (Central Counterparties, CCPs) und Zentralverwahrer (Central Securities Depositories, CSDs) sollte ausdrücklich ermöglicht werden. Die hohe Qualität und die bereits geltenden umfassenden regulatorischen Anforderungen für die bestehende Wertpapierverwahrung sollte auch für potenziell vergleichbar werthaltige und handelbare Security Token (wie künftig bspw. Real Estate-Token) Anwendung finden.

Soll ein Geschäft mit Security-Token, die sich als übertragbare Wertpapiere qualifizieren, an einem Handelsplatz ausgeführt werden, sind diese bei einem Zentralverwahrer einzubuchen, vgl. Art. 3 (2) CSDR. Wenn derartige Security-Tokens sich jedoch nur aufsichtsrechtlich, nicht aber depotrechtlich/zivilrechtlich als Wertpapier qualifizieren (wie derzeit bspw. BitBond), können sie jedoch bei einem CSD nicht eingeliefert werden, da sie - wie in dem RegE vorgesehen - bei einem Kryptoverwahrer zu verwahren sind und nicht bei einer Depotbank oder einem CSD. In der Folge können solche Security Tokens nicht handelbar gemacht werden. Das Clearing von solchen Security-Tokens durch einen Zentralen Kontrahenten würde gleichsam ein Verwahren und Verwalten beinhalten, diese Tätigkeiten dürften nach dem derzeitigen RegE allerdings nicht ausgeübt werden. Hier sollten Flexibilisierungen in den Entwurf aufgenommen werden.

3. Einfügen des Kryptoverwahrgeschäfts als Erlaubnistatbestand in das KWG

In § 1 Abs. 1a Satz 2 KWG wird in Nr. 6 das Kryptoverwahrgeschäft als neuer Erlaubnistatbestand i.S.e. Finanzdienstleistung eingefügt. Danach bedarf ein Dienstleister, der „die Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern und zu übertragen, für andere“ anbietet, zukünftig einer BaFin-Erlaubnis nach § 32 KWG.

Die Einfügung eines eigenen Erlaubnistatbestands erscheint aufgrund der Verlustrisiken sinnvoll, die sich für einen Nutzer ergeben können, der ihm zugeordnete Kryptowerte nicht selbst in einer eigenen Wallet verwahrt, sondern die Speicherung und Verwahrung seiner Private Keys einem Kryptoverwahr-Anbieter überlässt, wobei der Anbieter letztlich Zugriff auf die Private Keys des Nutzers erhält.

Auf S. 124 f. der Gesetzesbegründung des Regierungsentwurfs werden nunmehr Ausführungen dazu gemacht, was unter den einzelnen Tatbestandsvarianten „Verwahrung, Verwaltung und die Sicherung von Kryptowerten“ zu verstehen ist. „Verwalten ist im weitesten Sinne die laufende Wahrnehmung der Rechte aus dem Kryptowert.“ Eine Erläuterung, wie weit diese Verwaltung gehen kann, wäre hilfreich, da unter diese Begründung auch natürliche oder juristische Personen fallen könnten, die von ihren Kunden beauftragt sind, bspw. ein Stimmrecht auszuüben ohne selbst jemals Zugriff auf die Kryptowerte oder dazugehörigen Private Keys ihrer Kunden zu erhalten. Daneben könnte unter den Tatbestand der „Verwaltung von Kryptowerten“ auch die Tätigkeit von Unternehmen fallen (z.B. Portfolioverwalter), die für ihre Kunden andere Dienstleister als Kryptoverwahrer mit der eigentlichen Verwahrung/Speicherung von Private Keys in einem Sammelbestand oder auch einer „Omnibus-Wallet“ beauftragen. Die Unternehmen selbst haben keinen Zugriff auf Private Keys ihrer Kunden, da diese bei dem Kryptoverwahrer verwahrt oder gespeichert sind. Die Unternehmen führen dabei jedoch selbst Buch, welche Kryptowerte ihren Kunden zuzuordnen sind. Wir gehen davon aus, dass solche Unternehmen, die keinen Zugriff auf die Private Keys ihrer Kunden bekommen können, auch keine Kryptoverwahrung betreiben würden. Andernfalls wären solche Unternehmen u.U. Kryptoverwahrer auf erster Ebene und die Kryptoverwahrer, die die eigentliche Speicherung und Verwahrung von Private Keys übernehmen, wären Kryptoverwahrer auf zweiter Ebene bzw. „Unter-Kryptoverwahrer“. Eine Klarstellung wäre daher hilfreich, ob solche Unternehmen und die von ihnen für ihre Kunden beauftragten Kryptoverwahrer in eine quasi „Unter-Kryptoverwahrung“ oder Drittverwahrung bzw. Zwischen-Kryptoverwahrung laufen, wie es im klassischen Depotgeschäft möglich ist. Eine solche Konstruktion wäre zumindest auch mit Blick auf die Erlaubnispflichten unglücklich, wonach eine ausschließliche Erlaubnis für Kryptoverwahrer vorgesehen ist, die daneben keine weiteren Finanz- oder Bankdienstleistungen erbringen dürfen (s.o.).

Was Verwaltung i.S.d. Kryptoverwahrung bedeutet im Vergleich zur Verwaltung i.S.d. Depotgeschäfts, sollte unter Berücksichtigung der Funktionalitäten von Blockchain-Lösungen, Verwahrlösungen, Oracles und Smart Contracts etc. noch einmal konkretisiert werden.

Für uns stellt sich die Frage, wie die Verwahrung und Verwaltung von Kryptowerten/Private Keys in einer Welt mit verschiedenen Intermediären (Verwahrkette von Intermediären: CSD - Custodian – Banken - Kunden des Kunden - Endkunden etc.) in der Praxis aussehen soll. Nach dem derzeitigen RegE und einem weiten Anwendungsbereich des Begriffs der „Verwaltung“ würden „Unterverwahrer“ möglicherweise wie der CSD (als „Oberverwahrer“) eine Kryptoverwahrlizenz benötigen,

wenn sie ihrerseits Kryptowerte für ihre Kunden „verwalten“, was institutionelle Investoren und Marktinfrastrukturen von der „Unterverwahrung“ ausschließen würde. Insbesondere ein CCP und ein CSD sollte auch Private Keys für Banken durch einen Ausnahmetatbestand für CCPs und CSDs verwahren und verwalten dürfen. Eine Folge des RegE wäre, dass der Kryptowertemarkt stark beschränkt würde, da bspw. Kunden von Depot-Banken diese nicht für die Verwahrung von Kryptowerten nutzen könnten. Die Verwaltung von Kryptowerten für Banken in der Verwahrkette sowie zwischen Kryptoverwahrern sollte zulässig sein, da ansonsten der Banken-Retail-Markt ausgeschlossen wäre.

Dass Gesellschaften, die eine neue Kryptoverwahrlizenz beantragen, keine weitere Bank-, CCP-, oder CSD-Lizenz halten dürfen ist aus unserer Sicht nicht nachvollziehbar. Der RegE schließt so gerade etablierte, beaufsichtigte Finanzmarkt-Akteure (Banken, CCPs, CSDs) und deren Kundengruppen beim Thema Kryptowerte aus. Es erschließt sich uns nicht, warum gerade Finanzmarktakteure ausgeschlossen werden, Kryptowerte zu verwahren/verwalten, die umfangreiche Erfahrung mit dem Risikomanagement in anderen Assetklassen haben.

Offen ist auch, weswegen Kryptowerte nicht wie andere bereits bestehende Assetklassen (Commodity, Derivate...) behandelt werden sollten. Die vorgesehene aufsichtsrechtliche Trennung von Kryptowerten von anderen Assetklassen würde bedeuten, dass doppelte Infrastrukturen für Kryptowerte aufgebaut werden müssten und nicht alle Assets auf in Krisenzeiten bewährten Infrastrukturen abgewickelt werden können.

Der RegE bedeutet aus unserer Sicht in letzter Konsequenz, dass bestehende Marktinfrastrukturanbieter kein Clearing und Settlement von Kryptowerten durchführen dürften, da dies notwendig auch die Verwahrung und Verwaltung dieser Werte umfasst. Zudem wird der Mehrwert hinsichtlich der Verwahrung, Verwaltung und Abwicklung verschiedener Vermögenswerte auf einer Infrastruktur konterkariert, da unnötig fragmentiert, Strukturen verdoppelt und für die Zukunft beschnitten.

Andersherum bedeutet § 32 Abs. 1g KWG des Regierungsentwurfs dass eine Erlaubnis für das Kryptoverwahrgeschäft nur bekommt, wer daneben keine andere Bank- oder Finanzdienstleistung erbringt. Wer daneben eine andere KWG-erlaubnispflichtige Dienstleistung erbringen möchte, müsste seine Erlaubnis für das Kryptoverwahrgeschäft zurückgeben. Diese Regelung hat für einiges Aufsehen in der Branche gesorgt. In der Praxis wird ein Unternehmen, das z.B. Eigenhandel mit Kryptowerten betreiben möchte und zugleich eine Verwahrlösung für seine Kunden anbieten möchte, ein

Tochterunternehmen gründen müssen, das eine Erlaubnis für das Kryptoverwahrgeschäft beantragen kann.

Auf S. 125 der Gesetzesbegründung des Regierungsentwurfs wird zudem der Tatbestand der Sicherung näher ausgeführt: „Unter Sicherung ist sowohl die als Dienstleistung erbrachte digitale Speicherung der privaten kryptografischen Schlüssel Dritter, als auch die Aufbewahrung physischer Datenträger (z. B. USB-Stick, Papier), auf denen solche Schlüssel gespeichert sind, zu verstehen. Die bloße Zurverfügungstellung von Speicherplatz, z. B. durch Webhosting- oder Cloudspeicher-Anbieter, ist nicht tatbestandsmäßig, solange diese ihre Dienste nicht ausdrücklich für die Speicherung der privaten kryptografischen Schlüssel anbieten.“ Daneben heißt es weiter: „Nicht erfasst ist auch die bloße Bereitstellung von Hard- oder Software zur Sicherung der Kryptowerte oder der privaten kryptografischen Schlüssel, die von den Nutzern eigenverantwortlich betrieben wird, soweit die Anbieter keinen bestimmungsgemäßen Zugriff auf die damit gespeicherten Daten haben.“

Bei Geschäftsmodellen, bei denen die Private Keys eines Nutzers in Cloud-Anwendungen eines Anbieters gespeichert werden und der Nutzer Zugriff auf seine Private Keys durch Anmeldung in seinem beim Anbieter geführten Account erhält, wobei aufgrund von Verschlüsselungsmethoden der Anbieter selbst keinen Zugriff auf die Private Keys des Nutzers erhält, die jedoch letztendlich in einer Cloud gespeichert sind, die dem
Anbieter zugeordnet ist, bleibt offen, ob dieser Anbieter als Kryptoverwahrer einzuordnen ist oder nicht. Es könnte vom Tatbestand der Sicherung ausgegangen werden, da in einer dem Anbieter zugeordneten Cloud Private Keys für andere gespeichert werden. Andererseits soll durch die Art der Verschlüsselung gerade kein „bestimmungsgemäßer Zugriff“ auf die Private Keys der Nutzer durch den Anbieter erfolgen können. Einige Anbieter sehen hierbei Recovery Routinen für Private Keys vor. Eine Klarstellung, ob solche Geschäftsmodelle grundsätzlich vom Tatbestand der Kryptoverwahrung erfasst werden sollen, wäre hilfreich
Um hier Rechtssicherheit für Anbieter verschiedener Wallet-Lösungen zu schaffen, regen wir erneut an bspw. Einen Kriterien- oder Beispielkatalog für das Vorliegen des Kryptoverwahrgeschäfts zu veröffentlichen.

X. Umfang des Begriffs „Anbieter von Elektronischen Geldbörsen“ i.S.d. 5. Geldwäscherichtlinie

Die Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (Richtlinie (EU) 2018/843) sieht keine Definition oder genauere Beschreibung des Begriffs “Anbieter von elektronischen Geldbörsen” vor. Der Begriff ist zunächst neutral gefasst und könnte auch solche Anbieter erfassen, die wie Ledger eine Hardware Wallet anbieten sowie auch Anbieter die Software oder Desktop Wallets anbieten. Ob damit auch Wallet-Anbieter als geldwäscherechtlich Verpflichtete erfasst werden sollen, die Nutzern die Erstellung einer eigenen Wallet für Kryptowerte ermöglichen, wobei ausschließlich der Nutzer und nicht der Wallet-Anbieter Zugriff auf die Private Keys des Nutzers erhält, ist nicht ganz eindeutig.

Der Referentenentwurf sieht vor, dass “Anbieter von elektronischen Geldbörsen” als geldwäscherechtlich Verpflichtete zukünftig als Finanzdienstleister über den Tatbestand des “Kryptoverwahrgeschäfts” erfasst werden. Nach dem Wortlaut des Referentenentwurfs betreibt nur derjenige das Kryptoverwahrgeschäft, der „die Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern und zu übertragen, für andere“ erbringt. Sofern ein Nutzer seine Kryptowerte in einer eigenen Wallet speichert und der Wallet- Anbieter keinen Zugriff auf die in der Nutzer-Wallet gespeicherten Private Keys hat, wäre nach unserer Lesart der Anwendungsbereich des Kryptoverwahrgeschäfts nicht eröffnet. Ein Wallet-Anbieter bspw. einer Hardware-Wallet (z.B. Ledger) oder auch eines Wallet Clients wie MyEtherWallet, bei denen der Nutzer seine Private Keys selbst verwahrt, würden nicht von den geldwäscherechtlichen Pflichten erfasst.

Hier wäre in der Gesetzesbegründung eine Klarstellung wünschenswert, inwiefern – auch im Interesse einer Harmonisierung auf europäischer Ebene – der Anwendungsbereich der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie tatsächlich auf Wallet-Anbieter begrenzt sein soll, die für andere in Form des Kryptoverwahrgeschäfts Kryptowerte und Private Keys verwahren.

XI. Umsetzungsfrist oder Übergangsregelung für Betreiber des Kryptoverwahrgeschäfts

Die neuen Regelungen sollen bereits zum 1. Januar 2020 in Kraft treten. Für Unternehmen, die bereits jetzt das Kryptoverwahrgeschäft betreiben und auch die Voraussetzungen einer Erlaubnis erfüllen würden, wären Übergangsvorschriften sinnvoll. Andernfalls drohen diese Unternehmen, die bereits jetzt für große Investoren Vermögenswerte verwalten, ihr Geschäft vorübergehend einstellen zu müssen. Übergangsfristen, die beispielsweise vorsehen, dass Unternehmen, die bereits vor dem 1. Januar 2020 ihren Geschäftsbetrieb aufgenommen haben und bis zum [30. Juni 2020] einen Erlaubnisantrag bei der BaFin eingereicht haben, für einen gewissen Zeitraum ihr Geschäft auch ohne Erlaubnis weiter betreiben können.
Andernfalls droht eine Abwanderung von Vorreitermodellen ins Ausland, was für den Krypto-Standort Deutschland mehr Nachteile bringen würde.