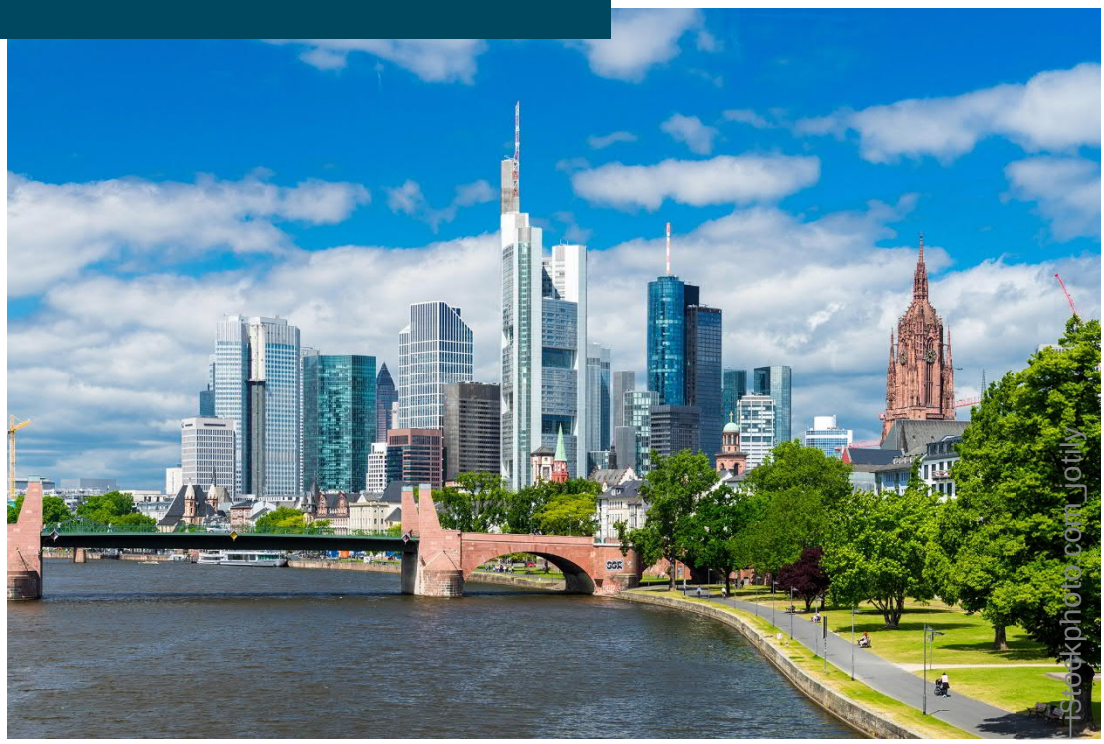
BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Auslegungs- und Anwendungs-hinweise

Besonderer Teil: Kreditinstitute



Inhaltsverzeichnis

Die vorliegenden Auslegungs- und Anwendungshinweise beziehen sich auf das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz; im Folgenden: GwG) in seiner Fassung vom 15. Januar 2021. Sie gelten für die Verpflichteten nach § 2 Abs. 1 Nr. 1 GwG. Soweit einzelne Punkte in diesem Besonderen Teil konkretisiert werden, geht der Besondere dem Allgemeinen Teil der Auslegungs- und Anwendungshinweise vor. Die Auslegungs- und Anwendungshinweise wurden schriftlich konsultiert, mit ihrer Veröffentlichung kommt die BaFin ihrem gesetzlichen Auftrag gemäß § 51 Abs. 8 GwG nach. Die Hinweise zu Ziffer 1 bezüglich der Herkunft der Vermögenswerte bei Bartransaktionen sind spätestens zwei Monate nach Veröffentlichung anzuwenden.

1. Herkunft der Vermögenswerte bei Bartransaktionen

Die Nationale Risikoanalyse (Bundesministerium der Finanzen, Erste Nationale Risikoanalyse – Bekämpfung von Geldwäsche und Terrorismusfinanzierung 2018/2019 – im Folgenden: NRA) macht deutlich, dass von Geschäften mit Bargeld (einschl. Sorten) und Edelmetallen als bargeldähnlichem Vermögenswert ein erhöhtes Risiko für Geldwäsche und Terrorismusfinanzierung ausgeht. Diesem Risiko ist angemessen zu begegnen. Hierbei ist zwischen Transaktionen innerhalb und außerhalb einer Geschäftsbeziehung (Bestands- und Gelegenheitskunden) zu differenzieren, da bei letzteren regelmäßig weniger Informationen zu dem Kunden vorliegen.

1.1 Außerhalb einer Geschäftsbeziehung

Bei Bartransaktionen, die von Kreditinstituten außerhalb einer Geschäftsbeziehung mit sogenannten Gelegenheitskunden durchgeführt werden, und die einen Betrag von 2.500,- Euro überschreiten, ist grundsätzlich ein erhöhtes Risiko i.S.d. § 15 Abs. 2 i.V.m. Anlage 2 GwG festzustellen. Aus diesem Grund sind gemäß § 15 Abs. 4 Nr. 2 GwG bei derartigen Bartransaktionen Informationen über die Herkunft der eingesetzten Vermögenswerte des Kunden sowie des gegebenenfalls vorliegenden wirtschaftlich Berechtigten vor Ausführung der Transaktion einzuholen. Ist die Durchführung der allgemeinen Sorgfaltspflichten in diesen Fällen nach dem GwG nicht zwingend, obliegt sie der Risikobeurteilung durch das Kreditinstitut. Die nach der Verordnung (EU) 2015/847 über die Übermittlung von Angaben bei Geldtransfers (im Folgenden: GeldtransferVO) bestehenden Pflichten bleiben hiervon unberührt.

Die Herkunft der Vermögenswerte ist durch die Vorlage eines aussagekräftigen Belegs zu plausibilisieren.

Wenn kein entsprechender Nachweis gemäß Ziffer 1.3 eingeholt werden kann, ist die Annahme des Bargelds abzulehnen.

1.2 Innerhalb einer Geschäftsbeziehung

Bei Bartransaktionen, die von Kreditinstituten innerhalb einer Geschäftsbeziehung (z.B. Bareinzahlung auf ein Kundenkonto) durchgeführt werden, und die einen Betrag von 10.000,- Euro überschreiten, ist grundsätzlich die Herkunft der Vermögenswerte durch aussagekräftige Belege nachzuweisen. Ziel dieses Nachweiserfordernisses ist die Plausibilisierung der Transaktion in der Zusammenschau mit den bereits über den Kunden vorliegenden Informationen. Der Nachweis kann innerhalb einer angemessenen Frist auch während der Geschäftsbeziehung persönlich vor Ort erbracht oder auf sonstige Weise übermittelt werden. Bei den Verfahren zur Übermittlung des Nachweises ist vom Kreditinstitut zu gewährleisten, dass die Information sicher und vertraulich übermittelt wird.

Bei Bartransaktionen bis 10.000,- Euro haben solche Maßnahmen nur auf risikobasierter Basis zu erfolgen.

Bei bestimmten Kundengruppen, bei denen regelmäßig höhere Bartransaktionen zum Geschäftsmodell gehören (z.B. Einzelhandel, der abends seine Tageskasse an Bargeldautomaten einzahlt), kann von diesem Grundsatz abgewichen werden, sofern die Bartransaktionen risikoorientiert regelmäßig auf Plausibilität geprüft werden.

1.3 Herkunftsnachweise

Aussagekräftige Belege als Herkunftsnachweis können insbesondere sein:

- Ein aktueller Kontoauszug bezüglich eines Kontos des (Lauf-)Kunden bei einer anderen Bank, aus dem die Barauszahlung hervorgeht
- ein aktueller Kontoauszug bezüglich des Kontos eines Dritten, aus dem die Barauszahlung hervorgeht (Handeln im Namen einer dritten Person), ergänzt um weitere Dokumente und Informationen zu dem Dritten,
- Barauszahlungsquittungen einer anderen Bank,
- Sparbücher des (Lauf-)Kunden, aus denen die Barauszahlung hervorgeht,
- Verkaufs- und Rechnungsbelege (z.B. Belege zum Autoverkauf, Goldverkauf),
- Quittungen bezüglich getätigter Sortengeschäfte,
- letztwillige vom Nachlassgericht eröffnete Verfügungen,
- Schenkungsverträge, Schenkungsanzeige.

Diese Aufzählung ist nicht abschließend. Insbesondere im Rahmen von Bartransaktionen innerhalb einer bestehenden Geschäftsbeziehung obliegt es der Beurteilung des Kreditinstituts, welche weiteren Belege als Herkunftsnachweise akzeptiert werden. Hierbei können die Art der Geschäftsbeziehung sowie besondere Umstände des Einzelfalls (beispielsweise Nachweise über Todesfall, Hochzeit, Geburtstag) angemessen berücksichtigt werden.

Der Nachweis ist nach Maßgabe des § 8 GwG aufzuzeichnen und aufzubewahren.

2. Immobilientransaktionen

Die NRA stuft das Geldwäscherisiko für den deutschen Immobiliensektor als hoch ein (NRA, Seite 103). Das Grundbuch schafft in Deutschland ein hohes Maß an Transparenz in Bezug auf die Eigentumsverhältnisse an Immobilien. Im Rahmen von sogenannten „Share Deals“ und

verschachtelten Gesellschaftskonstruktionen, insbesondere im Zusammenspiel mit Briefkastenfirmen aus dem Ausland, kann jedoch faktisch Anonymität hergestellt werden. Neben den typischerweise Beteiligten des Nichtfinanzsektors ist auch der Finanzsektor regelmäßig in diesem Kontext betroffen. Die NRA fordert daher besondere Wachsamkeit von Kreditinstituten, die im Rahmen solcher Transaktionen eingebunden werden oder in deren Ausgestaltung beratend tätig sind (NRA, Seiten 3, 103 f.).

Generell gilt, dass die nach dem GwG Verpflichteten über ein wirksames Risikomanagement gemäß § 4 GwG verfügen müssen. Im Rahmen der zu erstellenden Risikoanalyse müssen die Verpflichteten die Risiken der Geldwäsche und Terrorismusfinanzierung, welche aus den von ihnen angebotenen Geschäften mit Bezug zu Immobilientransaktionen herrühren können, ermitteln und bewerten. Durch angemessene interne Sicherungsmaßnahmen sind diese festgestellten Risiken zu steuern und zu mindern. Dazu gehört insbesondere die Schaffung von risikoorientierten, geschäftsinternen Prozessen, unterlegt mit den entsprechenden – bei Notwendigkeit verstärkten – Sorgfaltspflichten.

Eine wichtige Rolle bei der Risikoermittlung spielt das Erkennen von relevanten Sachverhalten. Die Kreditinstitute haben, je nach Art ihrer Einbindung in die Immobilientransaktion, risikoangemessene Maßnahmen zur entsprechenden Sachverhaltsaufklärung zu ergreifen. Hierbei können Typologien, die auf Geldwäsche oder Terrorismusfinanzierung hinweisen, hilfreich sein. Nicht abschließende Beispiele können im Einzelfall sein:

- Hinweise auf höhere Barzahlungen im Zusammenhang mit Immobilientransaktionen,
- (teilweise) Kaufpreiszahlung durch einen Dritten ohne plausiblen Grund,
- Immobilientransaktionen, bei denen der wirtschaftlich Berechtigte auf Käufer- oder Verkäuferseite nur schwer zu ermitteln ist (z.B. infolge undurchsichtiger Unternehmensstrukturen), insbesondere wenn ein Auslandsbezug besteht.

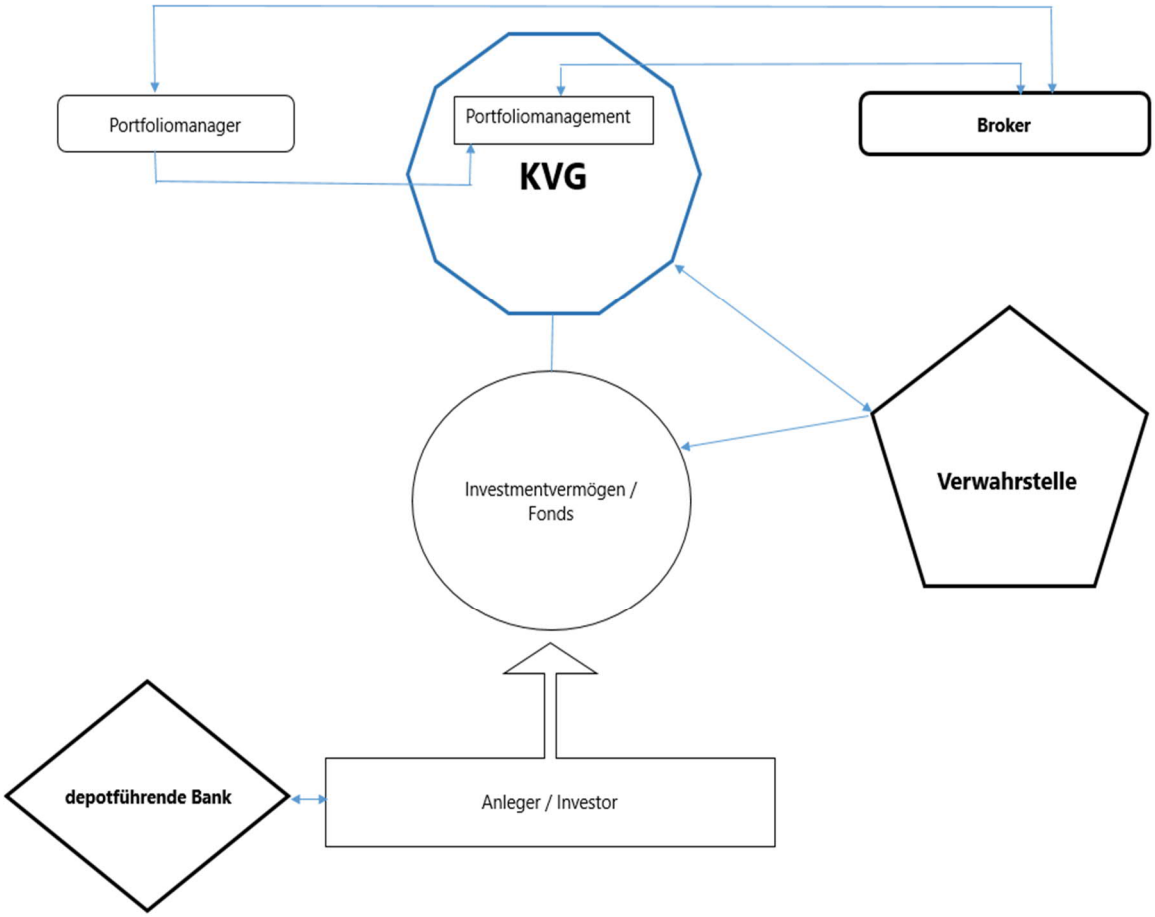
Für die Verpflichteten des Nichtfinanzsektors ergeben sich weitere Einzelheiten aus der Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich (Geldwäschegesetzmeldepflichtverordnung-Immobilien – GwGMeldV-Immobilien), BGBl. I Nr. 40, Seiten 1965 ff. vom 31.08.2020. Verpflichtete des Finanzsektors sind nicht Adressaten dieser Verordnung. Unter Umständen kann die Bestimmung von Sachverhalten im Immobilienbereich, die Meldepflichten für bestimmte Verpflichtetengruppen auslösen, Ausstrahlungswirkungen auf die Geldwäschepräventionssysteme anderer Verpflichteter i.S.d. § 2 Abs. 1 GwG entfalten.

Ergänzend sind von den Verpflichteten die jeweils aktuellen Hinweise und Typologiepapiere der Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit, im Folgenden: FIU) zu diesem Thema zu beachten und in die Risikobewertung einzubeziehen.

3. Investmentgeschäft

Kreditinstitute stehen in unterschiedlicher Weise in geschäftlicher Beziehung zu Fonds bzw. Investmentvermögen und deren Kapitalverwaltungsgesellschaften (im Folgenden: KVG), die sowohl im Inland als auch in EU-/EWR-Mitgliedstaaten oder in Drittstaaten ansässig sein können. Die Verwaltungsgesellschaften handeln im Interesse der Anleger des Investmentvermögens.

Grafik: Beteiligte im Investmentgeschäft



Die Bedrohung des Sektors, für Geldwäsche missbraucht zu werden, wird insgesamt als mittel eingestuft (NRA Seite 87). Allerdings ist insgesamt angesichts der heterogenen Strukturen eine differenzierende Betrachtung erforderlich.

Der BT Kreditinstitute geht nur auf Abklärungspflichten im Rahmen der allgemeinen Sorgfaltspflichten bei Geschäftsbeziehungen zu Verwaltungsgesellschaften von Investmentvermögen ein.

Neben der Pflicht festzustellen, ob ein Vertragspartner für einen wirtschaftlich Berechtigten handelt, haben Kreditinstitute nach § 10 Abs. 1 Nr. 3 GwG Informationen zu Art und Zweck der Geschäftsbeziehung einzuholen und zu bewerten.

Zur Bewertung des Risikos der Geschäftsbeziehung zur KVG ist den investmentrechtlichen Besonderheiten Rechnung zu tragen. Vor dem Hintergrund der - aus Gründen des Anlegerschutzes - vorgenommenen Aufspaltung zwischen der KVG und dem verwalteten Investmentvermögen, sind zur Beurteilung von Art und Zweck der Geschäftsbeziehung neben Informationen zur KVG auch Informationen zur Fonds- und Anlegerstruktur vom Kreditinstitut zu erheben. Hinsichtlich der Anlegerstruktur ist insbesondere abzuklären, ob es Anleger als wirtschaftlich Berechtigte am Investmentvermögen gibt.

Zur Feststellung der Identität der gegebenenfalls ermittelten Anleger ist zumindest deren Name und, soweit dies in Ansehung des im Einzelfall bestehenden Risikos der Geldwäsche oder der Terrorismusfinanzierung angemessen ist, weitere Identifizierungsmerkmale zu erheben. Die KVG muss dem Kreditinstitut die für dessen Risikobewertung erforderlichen Informationen zur Verfügung stellen. Das Kreditinstitut kann sich auf die seitens der KVG zur Verfügung gestellten Informationen verlassen, solange es keine begründeten Zweifel an deren Richtigkeit hat. Die gesamte Prüfung ist angemessen zu dokumentieren.

Bei offenen Publikumsinvestmentvermögen oder bei sonstigen Investmentvermögen mit einer Vielzahl von unmittelbaren und mittelbaren Anlegern darf angenommen werden, dass es aufgrund der Fonds- und Anlegerstruktur objektiv keinen Anleger als wirtschaftlich Berechtigten am Investmentvermögen gibt. In diesem Fall ist auch kein fiktiver wirtschaftlich Berechtigter gemäß § 3 Abs. 2 Satz 5 GwG zu erfassen. Bei einer Geschäftsbeziehung eines inländischen Kreditinstituts zu einer regulierten KVG oder einem regulierten Investmentvermögen mit Sitz in einem anderen EU-/EWR-Mitgliedstaat oder einem Drittstaat, deren Anforderungen an die Verhinderung, Aufdeckung und Bekämpfung von Geldwäsche und Terrorismusfinanzierung den FATF-Empfehlungen entsprechen, darf dies ebenfalls angenommen werden. Drittländer mit hohem Risiko nach der aktuellen Fassung der Delegierten Verordnung (EU) 2016/1675 entsprechen diesen Anforderungen nicht.

Ist weder die KVG noch das Investmentvermögen reguliert, kann sich der Umfang der Maßnahmen nach einem potentiell höheren Risiko für Geldwäsche und Terrorismusfinanzierung bestimmen.

4. Konsortialkredite

Im Rahmen von

- Konsortialfinanzierungen in der Ausgestaltung eines Außenkonsortiums,
- direkt gewährten Förderfinanzierungen („Direktgeschäft“) und
- Bürgschaftsfinanzierungen (d.h. Ermöglichung von Finanzierungen durch Bankverbürgung)

können die Konsorten/Finanzierungsbeteiligten/Förderbanken und Bürgschaftsbanken unter Beachtung der in § 17 Abs. 1-4 GwG genannten Regelungen auf den Konsortialführer bzw.

die „Hausbank“ als Dritten zur Erfüllung der kundenbezogenen Sorgfaltspflichten zurückgreifen.

Die Konsorten/die Förderbank sowie die Bürgschaftsbank, die zur Erfüllung der allgemeinen Sorgfaltspflichten gemäß § 10 GwG und Dokumentationspflichten nach § 8 GwG auf den Konsortialführer bzw. die „Hausbank“ zurückgreifen, haben insbesondere sicherzustellen, dass der Konsortialführer bzw. die „Hausbank“ die in § 17 Abs. 3 genannten Anforderungen erfüllt.

Sorgfaltspflichten sind vor der Beteiligung oder unter Beachtung der Vorgaben des § 11 Abs. 1 Satz 2 GwG und des § 25j Kreditwesengesetz (im Folgenden: KWG) im Zuge der Beteiligung an einem syndizierten Kredit/Konsortialkredit/Konsortialvereinbarung/Förderkredit zu erfüllen.

Der Konsortialführer/die „Hausbank“ hat die Konsorten/Beteiligten zu identifizieren. In der Regel können vereinfachte Sorgfaltspflichten nach § 14 GwG zur Anwendung kommen. Sofern es sich um eine reine Sicherheitenstellung für eine Finanzierung handelt, bei der nur ein geringes Risiko der Geldwäsche oder Terrorismusfinanzierung besteht, kann die Identifizierung entfallen.

5. Korrespondenzbankbeziehungen

Das Gesetz stellt in § 15 Abs. 3 Nr. 4, Abs. 7 i.V.m. § 1 Abs. 21 GwG besondere Anforderungen an „Korrespondenzbeziehungen“. Auf die Ausführungen in dem Kapitel III. Kundensorgfaltspflichten der BaFin-AuA-AT Ziffer 7.5 wird verwiesen.

Die folgenden Ausführungen konzentrieren sich auf Korrespondenzbeziehungen im Inter-Bankengeschäft, die im Folgenden als „Korrespondenzbankbeziehung“ bezeichnet werden. Eine Korrespondenzbankbeziehung stellt eine spezielle Art einer Geschäftsbeziehung im Sinne von § 1 Abs. 4 GwG zwischen einem Korrespondenten (Erbringer von Dienstleistungen) und einem Respondenten (Inanspruchnehmer von Dienstleistungen) dar. Sie liegt vor, wenn der Korrespondent innerhalb der Korrespondenzbeziehung (§ 1 Abs. 21 GwG) ein Verpflichteter gemäß § 2 Abs. 1 Nr. 1 GwG ist und für eine Respondenzbank Dienstleistungen im Sinne des § 1 Abs. 21 Nr. 1 oder Nr. 2 GwG erbringt. Typische Dienstleistungen sind etwa Dienstleistungen im internationalen Zahlungsverkehr, Scheckverrechnung oder Devisenhandelsdienstleistungen. Die bloße Führung eines Nostro-Kontos oder der bloße Austausch eines SWIFT-Schlüssels ohne Abwicklung von Zahlungen für die Respondenzbank begründen noch nicht die Stellung einer Korrespondenzbank (bzw. eines Korrespondenten) mit den daran anknüpfenden geldwäscherechtlichen Pflichten.

In der NRA wird betont, dass mit dem Korrespondenzbankgeschäft ein hohes inhärentes Risiko einhergeht (vgl. Seite 67). In Bezug auf die Gefahr, für Geldwäsche missbraucht zu werden, wurde es, im Vergleich mit anderen Produkten bzw. Dienstleistungen, bei den relevanten Instituten auf den ersten Plätzen eingeordnet.

Das Gesetz definiert für Korrespondenzbankbeziehungen einen Katalog obligatorischer Sorgfaltspflichten, die sich stets aus den allgemeinen Sorgfaltspflichten und, unter definierten

Voraussetzungen, zusätzlichen verstärkten Sorgfaltspflichten zusammensetzen. Die verstärkten Sorgfaltspflichten ergänzen den Katalog der allgemeinen Sorgfaltspflichten und bilden Mindestanforderungen. Unter risikoorientierter Bewertung des Einzelfalls sind sie gegebenenfalls um weitere Sicherungsmaßnahmen oder Sorgfaltspflichten zu ergänzen. Im Folgenden werden die gesetzlichen Anforderungen dargestellt und durch konkretisierende Hinweise ergänzt.

5.1. Sorgfaltspflichten

5.1.1 Allgemeine Sorgfaltspflichten

Im Rahmen jeder Korrespondenzbankbeziehung sind auf den Respondenten die allgemeinen Sorgfaltspflichten gemäß § 10 Abs. 1 GwG anzuwenden.

Folgende allgemeine Maßnahmen sind mindestens zu ergreifen:

- Die Identifizierung des Respondenten und gegebenenfalls der für ihn auftretenden Person(en) nach Maßgabe des § 11 Abs. 4 und des § 12 Abs. 1 und 2 GwG sowie die Prüfung, ob die für den Vertragspartner auftretende Person hierzu berechtigt ist. Anm.: Es besteht keine Verpflichtung der Korrespondenzbank, dass sie die Maßnahmen zur Feststellung und Überprüfung der Kundenidentität auf die Kunden der Respondenzbank anwendet oder die Daten dupliziert, die die Respondenzbank zu ihren Kunden eingeholt und dokumentiert hat. Kommt es im Rahmen der Überwachung einer Korrespondenzbankbeziehung zu Auffälligkeiten, kann es jedoch beispielsweise bei der Abklärung der auffälligen Transaktion(en) notwendig werden, Informationen zu einem oder mehreren Kunden des Respondenten bei dem Respondenten einzuholen.

- Die Abklärung des/der wirtschaftlich Berechtigten des Respondenten nach Maßgabe des § 11 Abs. 1 und 5 GwG; dies umfasst die Pflicht, die Eigentums- und Kontrollstruktur des Respondenten mit angemessenen Mitteln in Erfahrung zu bringen;

- die Einholung und Bewertung von Informationen über den Zweck und über die angestrebte Art der Geschäftsbeziehung, soweit sich diese Informationen im Einzelfall nicht bereits zweifelsfrei aus der Geschäftsbeziehung ergeben;

- die Feststellung mit angemessenen, risikoorientierten Verfahren, ob es sich bei dem/den wirtschaftlich Berechtigten um eine politisch exponierte Person (PeP), um ein Familienmitglied oder um eine bekanntermaßen nahestehende Person handelt, und

- die kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der Transaktionen, die in ihrem Verlauf durchgeführt werden, nach Maßgabe des § 25h Abs. 2 KWG zur Sicherstellung, dass diese Transaktionen übereinstimmen

- mit den beim Verpflichteten vorhandenen Dokumenten und Informationen über den Vertragspartner und gegebenenfalls über den/die wirtschaftlich Berechtigten, über deren Geschäftstätigkeit und Kundenprofil,
- soweit erforderlich, mit den beim Verpflichteten vorhandenen Informationen über die Herkunft der Vermögenswerte;

im Rahmen der kontinuierlichen Überwachung haben die Verpflichteten sicherzustellen, dass die jeweiligen Dokumente, Daten oder Informationen unter Berücksichtigung des jeweiligen Risikos in angemessenem zeitlichen Abstand aktualisiert werden.

Hierzu gehört auch die Überwachung der Einhaltung der sich aus der GeldtransferVO ergebenden Pflichten durch die Respondenzbank.

Unterhalten mehrere Banken innerhalb einer Gruppe Korrespondenzbankbeziehungen mit einer Respondenzbank, ist im Rahmen der gruppenweiten Pflichten (§ 9 Abs. 1 GwG) sicherzustellen, dass die Risikobewertungen der jeweiligen Banken mit der gruppenweiten Risikobewertungspolitik übereinstimmen und angemessene Informationsaustauschmechanismen eingerichtet sind. Gemäß § 9 Abs. 1 Satz 3 GwG ist sicherzustellen, dass die Korrespondenzbankbeziehung wirksam und koordiniert überwacht wird.

5.1.2 Verstärkte Sorgfaltspflichten

Ergänzend zu den allgemeinen Sorgfaltspflichten sind stets zusätzlich verstärkte Sorgfaltspflichten zu erfüllen, sofern:

- Es sich um eine grenzüberschreitende Korrespondenzbankbeziehung mit Respondenten mit Sitz in einem Drittstaat handelt,

- ein wirtschaftlich Berechtigter des Respondenten eine PeP ist,

- ein wirtschaftlich Berechtigter des Respondenten in einem von der Europäischen Kommission nach Artikel 9 der Richtlinie (EU) 2015/849 ermittelten Drittstaat mit hohem Risiko niedergelassen ist,

- es sich um eine Korrespondenzbankbeziehung mit Respondenzbanken in einem EWR-Staat handelt, die aufgrund einer Risikobeurteilung des Verpflichteten als erhöhtes Risiko beurteilt wurde. (Die Risikobeurteilung, dass ein höheres Risiko der Geldwäsche oder Terrorismusfinanzierung auch innerhalb des EWR besteht, kann im Rahmen der Risikoanalyse oder im Einzelfall unter Berücksichtigung der in den Anlagen 1 und 2 GwG sowie der in Leitlinie 8 der EBA Risk Factor Guidelines genannten Risikofaktoren erfolgen. Hilfreich können in diesem Zusammenhang ferner die Hinweise im Annex 2 Abschnitt II A. des Papiers „Sound management of risks related to money laundering and financing of terrorism“ des Baseler Ausschusses für Bankenaufsicht (Stand: Juni 2017) sowie in den Leitlinien der Financial Action Task Force (FATF) zu Korrespondenzbankdienstleistungen vom Oktober 2016 sein.) Eine solche institutsspezifische Risikobeurteilung ist stets vor Eingehung und anlassbezogen bzw.

periodisch während der Dauer einer Korrespondenzbankbeziehung vorzunehmen bzw. zu aktualisieren.

Zudem sind die Bewertungen der NRA in der institutsspezifischen Risikoanalyse und insbesondere bei der Entscheidung über die Anwendung der verstärkten Sorgfaltspflichten in Korrespondenzbankbeziehungen innerhalb des Europäischen Wirtschaftsraums angemessen zu berücksichtigen.

Unter den vorgenannten Voraussetzungen sind gemäß § 15 Abs. 7 GwG mindestens die folgenden verstärkten Sorgfaltspflichten kumulativ zu ergreifen:

1. Es sind ausreichende Informationen über den Respondenten einzuholen, um die Art seiner Geschäftstätigkeit in vollem Umfang verstehen und seine Reputation, seine Kontrollen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung sowie die Qualität der Aufsicht seines Sitzlandes bewerten zu können.

    a. Art der Geschäftstätigkeit:
    Das umfasst risikoangemessene Kenntnisse der Hauptgeschäftstätigkeit der Respondenzbank, einschließlich der Zielmärkte und Kundenarten in den wesentlichen Geschäftsbereichen.

    Das hierdurch erlangte Verständnis des Kundenportfolios des Respondenten sollte einem angemessenen fortlaufenden Abgleich mit den Ergebnissen der laufenden Überwachung der Geschäftsbeziehung mit dem Respondenten einschließlich des EDV-Monitorings der Zahlungsverkehrsabwicklung unterzogen werden.

    b. Reputation:
    Informationen über Mitglieder der Geschäftsleitung und Eigentümer der Respondenzbank, etwaige wirtschaftlich Berechtigte und ob in Bezug auf diese spezifische Geldwäsche- und Terrorismusfinanzierungsrisiken bestehen (z.B. als PeP oder mit Sitz in einem von der Europäischen Kommission nach Artikel 9 der Richtlinie (EU) 2015/849 ermittelten Drittstaat mit hohem Risiko).

    Informationen, ob von einem Gericht oder einer Aufsichtsinstanz zivil-, verwaltungs- oder strafrechtliche Maßnahmen oder Sanktionen, einschließlich öffentlicher Verwarnungen, gegen die Respondenzbank verhängt wurden, und falls ja, wie gravierend diese waren und ob die Respondenzbank die festgestellten Mängel behoben hat.

    c. Kontrollen:
    Informationen über die Richtlinien und Verfahren der Respondenzbank zur Prävention und Aufdeckung von Geldwäsche und Terrorismusfinanzierung, einschließlich einer Beschreibung der von der Bank auf ihre Kunden angewandten Maßnahmen zur Feststellung und Überprüfung der Kundenidentität und der Möglichkeit der Korrespondenzbank, Informationen zu einer bestimmten Transaktion zu erhalten.

d. Aufsichtsqualität:
   Informationen über die Qualität und Wirksamkeit der Bankenregulierung und -aufsicht im Land der Respondenzbank (insbesondere die Gesetze und Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung) und im Land des Mutterunternehmens, wenn es sich bei der Respondenzbank um ein verbundenes Unternehmen handelt. Hilfestellung können die Länderreports der FATF bieten.

2. Es ist vor Begründung einer Geschäftsbeziehung mit dem Respondenten die Zustimmung eines Mitglieds der Führungsebene einzuholen. Das Mitglied der Führungsebene der Korrespondenzbank ist regelmäßig und risikobasiert über die bestehenden Korrespondenzbeziehungen und die Ergebnisse ihrer laufenden Überwachung zu unterrichten.

3. Es sind vor Begründung einer solchen Geschäftsbeziehung die jeweiligen Verantwortlichkeiten der Beteiligten in Bezug auf die Erfüllung der Sorgfaltspflichten festzulegen, zu bestätigen und nach Maßgabe des § 8 GwG zu dokumentieren.

4. Es sind Maßnahmen zu ergreifen, um sicherzustellen, dass das Korrespondenzinstitut keine Geschäftsbeziehung mit einem Respondenten begründet oder fortsetzt, von dem bekannt ist, dass seine Konten von einer Bank-Mantelgesellschaft genutzt werden. Sofern sich die Korrespondenzbank hierzu eine entsprechende schriftliche Erklärung der Respondenzbank ausstellen lässt, hat sie diese mit angemessenen Mitteln zu überprüfen.

   Ergänzend sollte sich das Korrespondenzinstitut regelmäßig und risikoangemessen davon überzeugen, welche Sicherungssysteme der Respondent anwendet, um Mantelgesellschaften bzw. Briefkastenfirmen (shell companies) oder andere die Intransparenz fördernde Konstruktionen proaktiv zu erkennen und etwaigen Risiken daraus zu begegnen. Hierzu sind klare Kommunikationsvereinbarungen mit dem Respondenten empfehlenswert, vgl. auch Ziffer 3 zuvor.

5. Es sind Maßnahmen zu ergreifen, um sicherzustellen, dass der Respondent keine Transaktionen über Durchlaufkonten zulässt.

Die durchzuführenden Maßnahmen (7.5.3 BaFin-AuA-AT) sind im Rahmen von Korrespondenzbankbeziehungen von Seiten des Verpflichteten in Bezug auf das Respondenzinstitut zu erbringen. Die Pflicht erstreckt sich grundsätzlich nicht auf die Kunden des Respondenzinstituts, diese sind insbesondere keine wirtschaftlich Berechtigten im Rahmen der Korrespondenzbankbeziehung. Die Ausführungen zur risikoorientierten Anwendung verstärkter Sorgfaltsplichten, insbesondere bezüglich des Verständnisses des Kundenportfolios des Respondenten, bleiben hiervon unberührt.

Auf Respondenten mit Sitz in einem Drittstaat oder in einem Mitgliedstaat, bei dem nach der institutsspezifischen Risikoanalyse erhöhte Risiken angenommen werden, welche der gleichen Gruppe angehören wie der Verpflichtete und die der gruppenweiten Einhaltung geldwäscherechtlicher Pflichten unterliegen, sind die verstärkten Sorgfaltspflichten im Falle eines erhöhten Risikos anzuwenden.

5.2. Interne Sicherungsmaßnahmen

Gemäß § 25h Abs. 3 KWG sind die einzelnen Transaktionen im Zahlungsverkehr anhand des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und über die strafbaren Handlungen zu untersuchen, die im Verhältnis zu vergleichbaren Fällen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen.

Im Gegensatz zur gewöhnlichen Kundenbeziehung wird das Korrespondenzinstitut nur wenige Informationen über die Kunden seines Respondenten haben. Die Auffälligkeit einer Transaktion ist daher an den Informationen zu messen, die das Korrespondenzinstitut aufgrund des gesamten KYC-Prozesses über die Art und das Ausmaß der Geschäftstätigkeit sowie über das Kundenportfolio des Respondenten hat. Des Weiteren sollen die Informationen, welche im Zahlungsverkehr über die jeweiligen Transaktionen (einschließlich der Informationen über alle Beteiligten der Transaktion) übermittelt werden, einbezogen werden.

6. Monitoringsysteme

Gemäß § 25h Abs. 2 Satz 1 KWG müssen Kreditinstitute Datenverarbeitungssysteme betreiben, um Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die Anhaltspunkte für Geldwäsche, Terrorismusfinanzierung und sonstige strafbare Handlungen aufweisen.

6.1. Abgrenzung

Bei dem Betreiben von Datenverarbeitungssystemen ist grundsätzlich zwischen den beiden Komponenten Monitoring- und Screening-System zu unterscheiden.

- Monitoring ist die laufende ex-post Überwachung zur Auffindung ungewöhnlicher Transaktionen. Dies erfolgt nach deren Ausführung, um ungewöhnliche einzelne Transaktionen oder Transaktionsströme (beispielsweise Mustererkennung über die Abfolge von Transaktionen) zu erkennen. Zum Zeitpunkt des Erkennens einer Auffälligkeit im Monitoring ist die Zahlung somit bereits vollständig ausgeführt bzw. abgewickelt.

- Screening ist die Selektion oder das Herausfiltern vor allem von Zahlungsverkehrstransaktionen in Echtzeit, also noch vor deren Ausführung. Es soll unter anderem verhindern, dass Geldmittel trotz der Nichteinhaltung von Sanktionen, Embargos, des Verbots der Terrorismusfinanzierung oder anderer Maßnahmen verfügbar gemacht werden.

Im Folgenden wird grundsätzlich von „Datenverarbeitungssystemen“ gesprochen.

6.2. Angemessenheit

6.2.1 Auswahl und Beschaffenheit

Die Entscheidung, welches Datenverarbeitungssystem verwendet wird, und welche Geschäftsarten und Transaktionen unter Zugrundelegung der zuvor festgesetzten regelbasierten Indizien, Szenarien bzw. Parameter einer näheren Untersuchung unterfallen, hängt vom Umfang der Geschäftstätigkeit und von den Erkenntnissen der institutsspezifischen Risikoanalyse des jeweiligen Kreditinstituts ab. Die eingesetzten Bewertungsparameter, wann ein im Verhältnis zu vergleichbaren Fällen als ungewöhnlich einzuschätzender Sachverhalt vorliegt, sind anhand der institutsspezifischen Risikolage zu definieren (vgl. § 6 Abs. 1 Satz 2 GwG).

Das eingesetzte Datenverarbeitungssystem ist mit den relevanten Daten aus den relevanten IT-Systemen, d.h. vor allem Zahlungsverkehrs- und Transaktionssystemen, und den Kundenstammdatenbanken des Kreditinstituts zu versorgen. Jede Zahlungsverkehrstransaktion - intern, extern oder durchleitend – ist grundsätzlich durch das System zu prüfen. Jedoch können gewisse Fallkonstellationen ausgeschlossen werden, falls dem keine geldwäscherechtlichen Risiken entgegenstehen. Dies ist bei internen Buchungen zu bankeigenen Zwecken ohne Kundenbezug regelmäßig gegeben. Es ist sicherzustellen, dass die Ausschlüsse revisionssicher dokumentiert und mindestens jährlich auf ihre Angemessenheit überprüft werden.

Die persönliche Verantwortlichkeit des Geldwäschebeauftragten und des Vorstands für die Erfüllung der Pflicht nach § 43 GwG bleibt unberührt.

Um potentiell auffällige Geschäftsbeziehungen, Transaktionen oder Kontobewegungen aufzuspüren, muss das System auf die institutsspezifische Geschäftstätigkeit sowie die Kundenstruktur des Kreditinstituts ausgerichtet sein. Eine Anpassung der Parameter an die individuelle Risikosituation des Kreditinstitutes bzw. die institutseigene Risikoanalyse hat immer dann zu erfolgen, wenn die in der Risikoanalyse festgestellten Risiken nicht durch bereits vorhandene Indizien angemessen abgedeckt werden. Eine Anpassung kann auch in der Deaktivierung bestimmter Parameter bestehen. Anpassungen der Parameter müssen revisionssicher dokumentiert werden.

Das Datenverarbeitungssystem muss in seiner Gesamtheit in Bezug auf Daten, Konsistenz, Aktualität und Schnittstellen inhaltlich korrekt, vollständig und aktuell sein. Auch die Zuliefersysteme müssen in ihrer Gesamtheit in Bezug auf Daten, Konsistenz, Aktualität und Schnittstellen inhaltlich korrekt, vollständig und aktuell sein.

Das Datenverarbeitungssystem muss die generierten Treffer vollständig anzeigen (vgl. § 6 Abs. 1 Satz 2 GwG). Gewichtet das Datenverarbeitungssystem die Indizien, hat das Kreditinstitut eine angemessene Relevanzschwelle festzulegen, ab der Transaktionen als auffällig anzusehen sind und vom System angezeigt werden.

IT-basierte Entscheidungen des Datenverarbeitungssystems müssen erklärbar und nachvollziehbar sein. Es müssen die für das System und die generierten Treffer wesentlichen Einflussfaktoren aufgezeigt werden können und das Zustandekommen des Trefferergebnisses muss plausibel sein (Verbot von Blackboxen).

Bei fehlenden Daten sind die fehlenden Werte klar zu kennzeichnen und zeitnah durch Echtdaten zu ersetzen. Bis die Daten ersetzt wurden, sind risikosensitive default-Werte („Ersatzwerte“) zu setzen.

Das Datenverarbeitungssystem ist mit den für die einzelnen Indizien und Szenarien relevanten historischen Daten zu versorgen.

6.2.2 Geeignetheit der Software

Die für die Datenverarbeitungssysteme eingesetzte Software ist insbesondere dann geeignet, wenn sie

- das Kreditinstitut grundsätzlich in die Lage versetzt, Transaktionsmuster, Auffälligkeiten und Abweichungen zu erkennen,

- ein Indizienmodell enthält, das individuelle Konfigurierungen ermöglicht,

- neben Kunden- und Produktrisiken auch Länderrisiken (z.B. Verwendung aktueller Länderrisikolisten) und Terrorismusfinanzierungsrisiken (z.B. Verwendung aktueller Embargo- und Sanktionslisten; die Verwendung unterschiedlicher Software für die Datenverarbeitungssysteme im Hinblick auf Geldwäsche, sonstige strafbare Handlungen und Terrorismusfinanzierung sowie Sanktionsüberwachung ist zulässig) enthält,

- mit der Gesamtheit der verwendeten Indizien sowohl Aspekte der Geldwäscheprävention, der Prävention von Terrorismusfinanzierung, und – soweit geboten – der Verhinderung sonstiger strafbarer Handlungen, enthält,

- die erhöhten Risiken im Sinne des § 15 Abs. 3 GwG adäquat abdeckt,

- die Überprüfung von Namen auf Ähnlichkeiten mittels unscharfer Suchlogik („fuzzy logic“) im Rahmen des Sanktionsscreenings zulässt und

- Auswertungs- und Statistikfunktionen enthält oder von diesen unterstützt wird, die das Kreditinstitut in die Lage versetzen, Ad-hoc Recherchen durchzuführen und auf Auswertungen zur regelmäßigen Aktualisierung und Weiterentwicklung der Risikoanalyse zurückzugreifen. Auswertungs- und Statistikfunktionen können sich auch außerhalb der Datenverarbeitungssysteme befinden.

Die verwendeten Datenverarbeitungssysteme haben bei ihren Einstellungen, Regeln und Indizien unter Berücksichtigung der Risikolage des jeweiligen Kreditinstituts einschlägige Typologien im Bereich Geldwäsche, Terrorismusbekämpfung und sonstiger strafbarer

Handlungen abzudecken, um auffällige Kundenbeziehungen oder Transaktionen erkennen zu können. Darüber hinaus haben sie geeignete Szenarien vorzuweisen, die mindestens die aktuellen Erkenntnisse und Veröffentlichungen der FIU abbilden sowie weiteres öffentlich verfügbares Wissen über Geldwäsche, Terrorismusfinanzierung und sonstige strafbare Handlungen zugrunde legen.

Die Verwendung aller die gesetzlichen Vorgaben abbildenden Listen, insbesondere Sanktionslisten, Embargolisten und PeP-Listen, muss seitens der Datenverarbeitungssysteme gewährleistet sein. Sämtliche Listen müssen anlassbezogen bzw. regelmäßig überprüft und aktualisiert werden.

Die Möglichkeit von Peer-Group-Vergleichen (insbesondere bei großen Kundengruppen) ist bei Geeignetheit zu nutzen.

6.2.3 Funktionsfähigkeit der Datenverarbeitungssysteme

Die Richtigkeit und Aktualität der Indizien, Regeln, Schwellenwerte, Scores und Risikoklassifizierungssysteme muss unter besonderer Berücksichtigung aller relevanter gesetzlicher Änderungen, regulatorischer Vorgaben, Warnungen und Informationen regelmäßig und anlassbezogen überprüft werden.

Wesentliche Änderungen in der Risikoanalyse des Instituts sind in der Kalibrierung des Monitoring-Systems zu berücksichtigen.

Regelmäßige fachgerechte Wartung, Überholung und - soweit nötig - technische Aufrüstung der Hardware des Datenverarbeitungssystems zur Sicherung seiner Funktionsfähigkeit hat stattzufinden.

Die reibungsfreie Zusammenarbeit der Einzelkomponenten und deren Schnittstellen zu den Datenverarbeitungssystemen muss gewährleistet sein (End-to-End). Das Kreditinstitut hat die ordnungsgemäße Funktionalität der Datenverarbeitungssysteme laufend zu überprüfen und hat darüber hinaus regelmäßig für eine Qualitätskontrolle der Datenverarbeitungssysteme durch einen unabhängigen Prüfer zu sorgen. Diese Qualitätskontrolle kann im Rahmen der Jahresabschlussprüfung stattfinden.

Den Fall einer Störung oder des Ausfalls des Datenverarbeitungssystems hat das Kreditinstitut im Rahmen des Notfallkonzepts gemäß AT 7.3 der MaRisk zu berücksichtigen.

Änderungen der gesetzlichen Anforderungen hinsichtlich des Einsatzes von Datenverarbeitungssystem und deren Regelungsgegenstand sind unverzüglich nach deren Inkrafttreten umzusetzen.

6.2.4 Ordnungsgemäße und gesicherte Dokumentation

Die Indizien, Regeln, Szenarien, Kalibrierungen, Nutzer, deren Berechtigungen und entsprechenden Veränderungen sowie die Treffer und deren Bearbeitung inklusive dem geplanten weiteren Vorgehen (z.B. Erstattung einer Verdachtsmeldung bei der FIU) sind für einen sachkundigen Dritten in angemessener Zeit nachvollziehbar zu dokumentieren und im Sinne des § 8 GwG zu archivieren. Die Dokumentation der Trefferbearbeitung hat die inhaltliche Auseinandersetzung mit dem Einzelfall widerzuspiegeln. Veränderungen der Dokumentation sind nur dann zulässig, wenn sie als solche erkennbar sind und sich die entsprechenden Verantwortlichkeiten nachvollziehen lassen. Zusätzlich sind eine Begründung und der Zeitpunkt für eine solche Veränderung für einen sachkundigen Dritten nachvollziehbar zu dokumentieren.

6.2.5 Management, Personal und Berater

Es muss sichergestellt sein, dass die IT-Berechtigungsvergabe bei Datenverarbeitungssystemen im Sinne des AT 7.2 der MaRisk erfolgt. Aus dieser hat hervorzugehen, welche Personen mit der Trefferbearbeitung und Administrierung (inklusive Testen und Überprüfen) des Datenverarbeitungssystems befasst sind.

Die mit Zugangsberechtigungen ausgestatteten Personen (inklusive externer Berater) haben die erforderlichen fachlichen Qualifikationen und die nötige Expertise aufzuweisen. AT 7.1 Nr. 2 ist einschlägig.

Der Geldwäschebeauftragte ist für die fachliche Weiterentwicklung des Datenverarbeitungssystems, insbesondere die Änderung der vorhandenen Indizien, Regeln oder Szenarien, Schwellenwerte und Scores sowie deren Generierung und Kalibrierung verantwortlich und hat über entsprechende Kenntnisse zu verfügen. Die technische Umsetzung kann durch spezialisierte Mitarbeiter anderer interner oder externer Einheiten oder Dienstleister erfolgen.

Mit der Nutzung des Datenverarbeitungssystems betraute Mitarbeiter sind hinreichend zu schulen. Darüber hinaus ist eine fachliche Weiterbildung bei wesentlichen Veränderungen, wie z.B. der Generierung neuer Indizien oder Szenarien, erforderlich.

6.2.6 Freie Wahl hinsichtlich Datenverarbeitungssystem

Soweit die gesetzlich vorgegebenen und die oben aufgezeigten Kriterien erfüllt werden, sind die einzelnen Kreditinstitute hinsichtlich der Wahl des konkreten Datenverarbeitungssystems grundsätzlich ungebunden.

6.2.7 Absehen vom Einsatz eines Datenverarbeitungssystems

Kreditinstitute können vom Einsatz eines Datenverarbeitungssystems im Sinne von § 25h Abs. 2 Satz 1 KWG absehen, wenn sie über eine so geringe Anzahl von Vertragspartnern/wirtschaftlich Berechtigten oder Transaktionen verfügen, dass sie diese im Hinblick auf die darin liegenden Risiken auch ohne ein solches Datenverarbeitungssystem wirksam von Hand überwachen können. Eine Bilanzsumme von unter 250 Mio. Euro kann dabei grundsätzlich als Richtwert angesehen werden.

Förderbanken, Bausparkassen, Bürgschaftsbanken, Hypotheken- und Pfandbriefbanken können - unabhängig von der Höhe der Bilanzsumme - vom Einsatz eines Datenverarbeitungssystems absehen, wenn die in der institutsspezifischen Risikoanalyse bewertete Risikolage des Instituts dies zulässt.

Ein hinreichend geringes Risiko liegt vor, wenn das Spezialinstitut keine Zahlungskonten führt und Transaktionen überwiegend im Rahmen von nachgelagerten Geschäftstätigkeiten anfallen. Nachgelagerte Geschäftstätigkeiten bedeuten in diesem Zusammenhang insbesondere, dass Transaktionen ausschließlich über ein Konto des Kunden bei einem beaufsichtigten Kreditinstitut aus dem Europäischen Wirtschaftsraum von/an das Spezialinstitut erfolgen oder Transaktionen über das Bundesbankkonto des Spezialinstituts abgewickelt werden.

Kreditinstitute, die vom Einsatz eines Datenverarbeitungssystems absehen, müssen sich regelmäßig bestätigen lassen, dass das Absehen vom Einsatz eines Datenverarbeitungssystems uneingeschränkt angemessen ist. Eine Bestätigung durch einen Wirtschaftsprüfer z.B. im Rahmen der Jahresabschlussprüfung wird hierzu grundsätzlich als ausreichend angesehen.

6.2.8 Auslagerung ins Ausland (§ 6 Abs. 7 GwG i.V.m. § 25h Abs. 2 KWG und § 7 Abs. 5 GWG)

Kreditinstitute dürfen die Bearbeitung von Treffern eines Datenverarbeitungssystems durch einen Dritten durchführen lassen.

Kreditinstitute dürfen nicht auf einen Dritten zurückgreifen, der in einem Drittstaat mit hohem Risiko niedergelassen ist.

Es ist sicherzustellen, dass der Geldwäschebeauftragte Zugriff auf alle Treffer hat und unverzüglich über relevante Treffer informiert wird, so dass die Zeitvorgaben für die Abgabe von Verdachtsmeldungen eingehalten werden.

Die Durchführung einer internen Sicherungsmaßnahme gemäß § 6 Abs. 7 GwG stellt eine wesentliche Auslagerung im Sinne des § 25b KWG dar.

7. (Sammel-)Treuhandkonten

7.1 Grundsätze

Zur Abklärung der wirtschaftlich Berechtigten gelten die Vorgaben des Kapitels 5.2 der BaFin-AuA-AT bei Treuhandkonten entsprechend. Aufgrund des bestehenden Risikopotentials hat die gemäß § 10 Abs. 1 Nr. 2 i.V.m. § 11 Abs. 5 GwG erfolgende Abklärung und Identifikation des wirtschaftlich Berechtigten bei Treuhandkonten risikobasiert zu erfolgen.

Besondere Bedeutung hat in diesem Zusammenhang die Verdachtsmeldepflicht nach § 43 Abs. 1 Nr. 3 GwG bei Verstoß gegen die Offenlegungspflicht nach § 11 Abs. 6 Satz 3 GwG.

7.2 Ausnahmen für bestimmte Fallgruppen

Auch wenn (Sammel-) Treuhandkonten grundsätzlich ein besonderes Geldwäscherisiko aufweisen können, gibt es enge Ausnahmen, in denen das Risiko geringer ausfallen kann:

7.2.1 Anwendung vereinfachter Sorgfaltspflichten bei bestimmten Sammelkonten

Kreditinstitute können bei Sammeltreuhandkonten für bestimmte Fallgruppen aufgrund risikoorientierter Entscheidung vereinfachte Sorgfaltspflichten gemäß § 14 GwG anwenden. Das hat zur Folge, dass den Pflichten zur Abklärung des wirtschaftlich Berechtigten dadurch nachgekommen werden kann, dass der Treuhänder auf Verlangen des Instituts eine Liste der aktuellen wirtschaftlich Berechtigten vorlegt. Vereinfachte Sorgfaltspflichten können bei Sammeltreuhandkonten mit niedrigem Risiko wie Konten für beispielsweise Klassenkassen, Kegelclubs, Heimbewohnern oder ähnlichen Konstellationen in Betracht kommen. Dies kann je nach Einzelfall auch für Inkassounternehmen gelten, wobei hier die Risikoeinstufung des Vertragspartners zu berücksichtigen ist (z.B. möglich bei Inkassoleistungen im Gesundheitswesen).

Darüber hinaus können bei Sammeltreuhandkonten von Kunden, die selbst Verpflichtete nach dem GwG sind und unter Aufsicht der Bundesanstalt stehen, - vorbehaltlich einer entgegenstehenden Risikobeurteilung durch das Kreditinstitut - vereinfachte Sorgfaltspflichten anwendbar sein. Diese Risikobeurteilung muss dem spezifischen Geschäftsmodell des Kunden entsprechend angemessen erfolgen.

7.2.2 Keine Feststellung der wirtschaftlich Berechtigten bei Treuhandkonten im Falle der Insolvenz, Testamentsvollstreckung und Zwangsverwaltung

In den Fällen, in denen dem Eigentümer jegliche Einflussnahmemöglichkeit auf die Verwaltung und Verwertung des betroffenen Vermögens kraft Gesetz entzogen ist, kann keine Veranlassung i. S. d. § 3 Abs. 1 Nr. 2 GwG an den entsprechenden Konten vorliegen.

Beispiele hierfür sind Insolvenz, Testamentsvollstreckung und Zwangsverwaltung. Entsprechend kann kein „wahrer“ wirtschaftlich Berechtigter vorliegen. Der Erfassung des Insolvenz- bzw. Zwangsverwalters oder Testamentsvollstreckers als „fiktiver“ wirtschaftlich Berechtigter des Schuldners bedarf es nicht, weil dieser bereits entweder als Kontoinhaber oder als Verfügungsberechtigter hinterlegt ist.

8. Trade Finance

8.1 Allgemeines

Unter Trade Finance versteht man die Finanzierung und Absicherung des Außenhandels der Nichtbanken mit Hilfe von Kreditinstituten. Die NRA sieht in diesem Bereich aufgrund der komplexen Strukturen und des Auslandsbezuges ein erhöhtes Risiko für Geldwäsche und Terrorismusfinanzierung in Deutschland. Grund hierfür ist die Rolle Deutschlands als weltweit drittgrößter Warenexporteur und -importeur und die insoweit generierten hohen Handelsvolumina. Diesem erhöhten Risiko ist durch ausreichende Kenntnisse über das zugrundeliegende Handelsgeschäft sowie die Geschäftspartner zu begegnen, um so Hinweise für handelsbasierte Geldwäsche zu erkennen (NRA, Seiten 66f.).

In diesem Bereich haben sich international anerkannte Branchenstandards herausgebildet, insbesondere die Uniform Customs & Practice for Documentary Credits (600) der International Chamber of Commerce (ICC).

Darüber hinaus sollten die EBA Risk Factor Guidelines, insbesondere die Ausführungen unter Leitlinie 13, Beachtung finden.

Im Bereich Trade Finance unterscheidet man – neben Krediten für mittel- und langfristige Finanzierungen - zwischen kurzfristigen, nicht-dokumentären Zahlungsinstrumenten (z.B. Auslandsüberweisungen) und kurzfristigen, dokumentär gesicherten Zahlungsinstrumenten (z.B. Dokumenteninkasso und Akkreditiv). Die folgenden Ausführungen beziehen sich auf die kurzfristigen, dokumentären Formen des Trade Finance Geschäftes.

8.2 Sorgfaltspflichten

Transaktionen in diesem Bereich sind ebenso wie alle anderen Geschäftsbeziehungen eines Kreditinstituts geldwäscherechtlichen Prüfungen zu unterziehen. Insbesondere sind kundenbezogene Sorgfaltspflichten zu erfüllen.

Zu diesem Zweck soll das Kreditinstitut, das Dienstleistungen im Bereich des Trade Finance erbringt, ein Verständnis für die Geschäftstätigkeit seiner Kunden entwickeln, um auf diese Weise ungewöhnliche oder verdächtige Transaktionen identifizieren zu können. Hierzu können insbesondere Informationen bezüglich

- der Länder, in denen der Kunde Geschäfte betreibt,
- der Handelsrouten, die genutzt werden,

- der Waren, mit denen der Kunde handelt,
- den Geschäftspartnern, mit denen der Kunde Handel treibt und
- dem Umstand, ob der Kunde auf Vertreter oder Dritte zurückgreift und wo diese ihren Sitz haben

herangezogen werden.

Abhängig von der Risikobeurteilung des Kreditinstituts können auch vereinfachte oder verstärkte Sorgfaltspflichten angezeigt sein. Bei seiner Risikobeurteilung sollte das Kreditinstitut zusätzlich transaktionsbezogene, kundenbezogene und/oder geographische Faktoren beachten, die das Ausmaß des Risikos beeinflussen können. Beispiele für solche Faktoren finden sich in den EBA Risk Factor Guidelines.

Soweit aufgrund der Risikobeurteilung des Kreditinstituts verstärkte Sorgfaltspflichten anzuwenden sind, ist eine gründliche Überprüfung der beteiligten Parteien sowie eine angemessene Überwachung der Transaktion angezeigt.

Im Rahmen der Prüfung der beteiligten Parteien sollte das Kreditinstitut Informationen über die Eigentümer und die Vorgeschichte der einzelnen Beteiligten einholen, z.B. durch Abfrage von Handelsregistern, Erkundigung bei Drittquellen und öffentlichen Internetquellen. Die Aufbewahrung der SWIFT-Nachrichten kann – abhängig von der Risikobeurteilung – als Dokumentation ausreichen.

8.3 Besonderheiten bei der Transaktionsüberwachung

Einzelne Transaktionen sind unter Berücksichtigung der Risikobeurteilung und der dabei beachteten Faktoren auf Plausibilität zu prüfen. Hierbei können unter anderem folgende Anhaltspunkte hilfreich sein:

- Stimmigkeit zwischen ausgewiesenem Warenwert und Marktwert,
- Stimmigkeit des Lieferumfangs, des Kontrahenten- und Lieferlandes und der Transport- und Zahlungswege im Vergleich zum üblichen Geschäftsgebaren des Kunden, seiner Vergleichsgruppe und der Marktsituation sowie der zuvor getätigten Angaben.

Die Überwachung erfordert hier regelmäßig mehr manuellen Aufwand als bei herkömmlichen Kundenzahlungen, da die Absicherung von Außenhandelsgeschäften, insbesondere Akkreditivgeschäften, in der Regel dokumentenbasiert abgewickelt wird. Es ist sicherzustellen, dass die Dokumente, die dem Kreditinstitut im Zuge einer Absicherung von Außenhandelsgeschäften vorgelegt werden, auch auf ihre Stimmigkeit mit den international anerkannten Richtlinien (ERA/ERI) geprüft werden. Dies kann risikoorientiert erfolgen. Besonderes Augenmerk ist auf Dokumente zu legen, welche nicht den international üblichen Gepflogenheiten entsprechen.