Umgang mit dem Geldwäschegesetz- Eckpunkte für ein wirksames AML-Risikomanagment.

Richtlinien für die Etablierung von Abläufen zur Kundenannahme und -überwachung

COMPANY.INFO

CMS law·tax·future

Inhaltsangabe.

Was Ihnen dieses Handbuch liefert 3

Experten 4

Das GwG: Hintergrund und Anwendungsbereich 6

Besteht in Ihrem Unternehmen bereits Grundwissen über das Geldwäschegesetz („GwG“) und die anwendbare Verwaltungspraxis?
Dann können Sie auf Seite 10 zu den zehn Schritten einer Know Your Customer („KYC“)-Prüfung springen. Dort finden Sie hilfreiche Tipps zu Einrichtung und Optimierung eines wirksamen Risikomanagements sowie Praxisbeispiele zu typischen Problemfeldern.

Die richtigen Grundlagen 10

1. Festlegung von Verantwortlichkeiten 10
2. Erstellung einer Risikoanalyse und Festlegung von Methoden 11
3. Erstellen eines Schulungsplans 14
4. Effiziente Aufzeichnung und Aufbewahrung von KYC-Daten 14

Die zehn Schritte der KYC-Prüfung 15

1. Identifizieren Sie den Kunden. 16
2. Überprüfen Sie die Kundenidentität. 16
3. Stellen Sie fest, ob eine Stellvertretung vorliegt. 17
4. Stellen Sie den Zweck und die beabsichtigte Art der Geschäftsbeziehung fest. 17
5. Recherchieren Sie woher das Vermögen und die Ressourcen stammen. 17
6. Verschaffen Sie sich Einblicke in die Eigentums- und Kontrollstruktur des Kunden. 18
7. Stellen Sie fest, ob es sich beim Kunden oder dem UBO um eine PEP handelt. 22
8. Führen Sie zu Kunden zu Übereinstimmungen mit Sanktionslisten und negativer Presseberichterstattung durch. 23
9. Führen Sie den Kunden einer Risikokategorie zu. 24
10. Überprüfen Sie Kunden in risikoangemessenen Abständen. 28

Der rote Faden: Überwachen Sie Geschäftsbeziehungen sorgfältig und automatisieren Sie Prozesse, wo möglich 32

Was Ihnen dieses Handbuch liefert.

Vom Steuerberater, Immobilien- oder Güterhändler bis zum Finanzinstitut: Zahlreiche Personen und Unternehmen in Deutschland unterliegen dem Geldwäschegesetz (GWG). Das Gesetz benennt eine Reihe von Sorgfaltspflichten, die gegenüber Kunden, aber auch intern einzuhalten sind. Vorgaben, die mit großem Aufwand und oft Unsicherheit verbunden sind. Dieses Handbuch bietet Ihnen viele Tipps und Checklisten, die Ihnen bei der Implementierung und Umsetzung helfen.

Eine der Herausforderungen des GwG ist der risikobasierte Ansatz. Die „Verpflichteten" (Personen oder Unternehmen mit geldwäscherechtlichen Pflichten) müssen die Anforderungen an das konkrete Risikoprofil eines Kunden, eines Produktes oder einer Transaktion anpassen. Die Risikoeinschätzung obliegt dabei dem Verpflichteten, ebenso wie die konkrete Umsetzung des Pflichtenkatalogs.

Eine weitere Hürde: Die Anforderungen des GwG werden immer mehr. Als die vierte Geldwäscherichtlinie für erheblichen Änderungsbedarf im GwG sorgte, stand bereits die Änderungsrichtlinie zur Vierten Geldwäscherichtlinie („Fünfte Geldwäscherichtlinie") in den Startlöchern. Auch der Straftatbestand der Geldwäsche erfuhr 2021 weitreichende Änderungen. Aktuell liegt der Entwurf eines umfassenden Regelungspakets der EU bereit, wonach ein Großteil der Regelungen der Fünften Geldwäscherichtlinie in eine Verordnung transferiert werden könnte.

Um die Umsetzung zu vereinfachen, haben Aufsichtsbehörden Auslegungs- und Anwendungshinweise veröffentlicht (die so genannte Verwaltungspraxis). Für den Finanzsektor maßgeblich sind die Hinweise der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin AuA"). Für Kreditinstitute wurden diese durch einen besonderen Teil ergänzt. Auf europäischer Ebene veröffentlicht die europäische Bankenaufsichtsbehörde (European Banking Authority – „EBA") regelmäßig Leitlinien zur Umsetzung geldwäscherechtlicher Vorgaben.

Dennoch ist es nach wie vor schwierig, den risikobasierten Ansatz in die Praxis umzusetzen.

Eine Übersicht, die Licht ins Dunkel bringt

Auf den nächsten Seiten erhalten Sie einen Überblick über die wesentlichen Änderungen, die das GwG im Laufe der Jahre erfuhr. Wir zeigen Ihnen, wie Sie die aktuellen Vorgaben am besten umsetzen und werfen einen Blick in die Praxis.

So finden Sie Praxistipps zu typischen Problemfeldern, etwa der Identifikation von Strohmännern, dem Umgang mit komplexen Gruppenstrukturen oder der Risikoklassifizierung von Kunden.

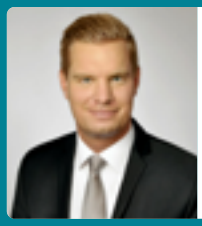
Darüber hinaus bieten wir Orientierungspunkte für die effiziente Ausgestaltung eines Geldwäsche-Risikomanagements. Dabei können Ihnen Datenbanken sehr von Nutzen sein. Diese helfen Ihnen, Kunden zeitnah und präzise zu überwachen. Diese Datenbanken liefern Ihnen hilfreiche Informationen zur effizienteren Umsetzung des GwG-Pflichtenkatalogs nach dem GwG und sparen damit viel Zeit.

Experten.

Dieses Handbuch wurde in Zusammenarbeit mit folgenden Experten und Partnern erstellt.

Dr. Joachim Kaetzler
Rechtsanwalt, Partner, CMS Germany

Charlotte Salathé
Rechtsanwältin, Senior Associate, CMS Germany



Till Komma
Rechtsanwalt, Senior Associate, CMS Germany

Daniel Brunzema
Country Manager Deutschland, Company.info

Die Herausforderungen von heute und morgen verlangen mutige, unabhängig denkende Persönlichkeiten, die in der Gemeinschaft so vielfältig sind wie die Problemstellungen unserer Mandanten. Während sich die Welt neu erfindet, komplexer wird, schnellere Reaktionen erfordert, stehen wir für Ihre Interessen ein und formen sie an Ihrer Seite mit.

Mehr als 600 Rechtsanwälte, Steuerberater und Notare in acht Büros entwickeln rechtssichere Lösungen für Mandanten – von Start-ups über mittelständische Unternehmen bis hin zu multinationalen Großkonzernen. Die Anwälte von CMS in Deutschland bringen nicht nur die notwendige fachliche Spezialexpertise auf allen Gebieten des Wirtschaftsrechts mit, sondern kennen auch die marktspezifischen Anforderungen in sämtlichen Industriezweigen und Branchen.

Eine lösungsorientierte Beratung am Puls der Zeit, geprägt durch ein äußerst innovationsfreudiges Team ist das Leistungsversprechen von CMS an Sie. Denn wir glauben: Wer gestalten und die Herausforderungen annehmen will, muss etwas wagen und neue Perspektiven einnehmen. Um neue Lösungen zu entwickeln für unerwartete Fragestellungen. Um weiter zu gehen als jemals zuvor.

International vertreten. Direkt bei Ihnen vor Ort

CMS ist eine der größten Wirtschaftskanzleien weltweit. Mehr als 4.800 Juristinnen und Juristen arbeiten in grenzüberschreitenden Teams zusammen. In 71 Städten in 43 Ländern setzen wir uns mit der gleichen Leidenschaft und dem gleichen Qualitätsanspruch für die Ziele unserer Mandanten ein.

Damit ist CMS optimal aufgestellt, um Ihnen genau das rechtliche und steuerrechtliche Know-how und die regionale Marktkenntnis zu bieten, die Sie benötigen, um Ihre unternehmerischen Ziele zu erreichen und sich im Wettbewerb zu behaupten – wo immer Sie geschäftlich aktiv sind.

World Law Groep

In Ländern, in denen wir keine eigenen Büros unterhalten, verfügen wir über etablierte Beziehungen zu lokalen Kanzleien und konkreten Ansprechpartnern der World Law Group, mit denen wir seit 1988 zusammenarbeiten und deren Fachkenntnis und Qualität wir daher garantieren können.

Das GwG: Hintergrund und Anwendungsbereich.

Das GwG setzt im Wesentlichen die Anforderungen der EU-Geldwäscherichtlinien um. Diese wiederum basieren weitgehend auf den Empfehlungen der Financial Action Task Force („FATF"), ein zwischenstaatliches Gremium, das internationale Standards im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung setzt und regelmäßig Empfehlungen hierzu formuliert („FATF-Empfehlungen"). Die 2003 durchgeführte Erweiterung der FATF-Empfehlungen hat zur Verfassung und Annahme der Dritten Geldwäscherichtlinie geführt. 2008 wurde diese Dritte Geldwäscherichtlinie in deutsches Recht umgesetzt. Mit der Umsetzung dieser Richtlinie wurde das damalige GwG gänzlich überarbeitet und vollständig neugefasst.

Adressaten der geldwäscherechtlichen Pflichten sind Unternehmen des Finanz- und des Nichtfinanzsektors, die abschließend im Katalog des § 2 Abs. 1 GwG aufgeführt werden. Eine vereinfachte Übersicht über die Verpflichteten finden Sie nachfolgend.

Verpflichtete nach dem GwG

Unternehmen des Finanzsektors
Kreditinstitute (hierzu zählen auch Bausparkassen, deren Geschäftsbetrieb darauf gerichtet ist, Einlagen von Bausparern (Bauspareinlagen) entgegenzunehmen und aus den angesammelten Beträgen den Bausparern für wohnungswirtschaftliche Maßnahmen Gelddarlehen (Bauspardarlehen) zu gewähren (Bauspargeschäft))
Finanzdienstleistungsinstitute (Unternehmen, die ohne Kreditinstitute zu sein, Finanzdienstleistungen nach § 1 Abs. 1a KWG erbringen)
Wertpapierinstitute
Zahlungsinstitute und E-Geld-Institute (insbesondere auch Anbieter von Zahlungsauslösediensten sowie von Kontoinformationsdiensten)
Agenten und E-Geld-Agenten im Sinne des Zahlungsdiensteaufsichtsgesetzes (ZAG)
Finanzunternehmen (legaldefiniert in § 1 Abs. 24 GwG)
Versicherungsunternehmen / -vermittler, die bestimmte Katalogprodukte anbieten bzw. vermitteln
Kapitalverwaltungsgesellschaften
sowie im Inland gelegene Zweigstellen und Zweigniederlassungen dieser Unternehmen mit Sitz im Ausland

Unternehmen des Nicht-Finanzsektors (Personen, juristische Personen oder Gesellschaften, die im Rahmen ihres Gewerbes oder Berufs handeln)
Rechtsanwälte, Syndikusrechtsanwälte, Kammerrechtsbeistände, Patentanwälte und Notare (im Rahmen der Ausübung bestimmter Katalogtätigkeiten)
Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater, Syndikussteuerberater und Steuerbevollmächtigte
Dienstleister für Gesellschaften und Treuhandvermögen und Treuhänder
Immobilienmakler
Veranstalter und Vermittler von Glücksspielen
Güterhändler, Kunstvermittler und Kunstlagerhalter

Die wesentlichen Änderungen im Überblick

Innerhalb der Geschichte des GwG wurde dieses bereits vielfach angepasst und geändert. Hintergrund ist stets die Umsetzung von Vorgaben des EU-Richtliniengebers. Im Mai 2015 wurde die Vierte Geldwäscherichtlinie verabschiedet. Im Jahr 2018 folgte die Änderungsrichtlinie zur Vierten Geldwäscherichtlinie, auch Fünfte Geldwäscherichtlinie genannt. Anfang des Jahres 2020 erfolgte die Umsetzung dieser Richtlinie auf deutscher Ebene. Mit der Umsetzung gingen die Aktualisierung des Gesetzes, jedoch auch eine Verschärfung in einigen Teilbereichen einher. Auf der unten gezeigten Zeitachse sind die wichtigsten Änderungen in chronologischer Reihenfolge aufgeführt.

1993
Die Urform des GwG

Das GwG in seiner Urform wurde am 29.11.1993 als eigenständiges Sondergesetz in die deutsche Rechtsordnung aufgenommen. Hintergrund war die Umsetzung der Anforderungen der Ersten Geldwäscherichtlinie in nationales Recht.

2002
Ergänzung um Terrorismusfinanzierung

- Ergänzung des GwG durch das Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz).
- Erstmals muss eine Verdachtsmeldung auch dann vorgenommen werden, wenn Tatsachen auf die Finanzierung einer terroristischen Vereinigung schließen lassen.
- Ebenso wurden erstmals einige freie Berufe als Verpflichtete aufgenommen.

2008
Vollständige Überarbeitung

- Auf der Grundlage der Dritten Geldwäscherichtlinie wurde das Geldwäschegesetz mit dem Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz) vollständig überarbeitet und neu strukturiert.
- Eingeführt wurden unter anderem verstärkte Sorgfaltspflichten bei sogenannten politisch exponierten Personen (Politically Exposed Person – „PEP“).
- Der Begriff des wirtschaftlich Berechtigten wurde näher konkretisiert.
- Der regelbasierte Ansatz wurde durch den risikobasierten Ansatz ersetzt.

Änderungen und Anpassungen in den Folgejahren

- In den folgenden Jahren wurde das GwG vielfach punktuell geändert, insb. der Deutschland-Bericht der FATF im Jahr 2010 zog umfangreichen Änderungsbedarf nach sich.
- So wurde es beispielsweise um eine Erweiterung im Bereich des Glücksspiels ergänzt.
- Zudem wurde die Schwelle zur Abgabe einer Verdachtsmeldung herabgesetzt.
- Im Übrigen erfolgten kleinere Änderungen sowie redaktionelle Anpassungen.

2017
Umfangreiche Erweiterungen

- Die Umsetzung der Vierten Geldwäscherichtlinie führte zu erheblichen Erweiterungen des GwG.
- Die Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit – „FIU“) wurde vom Bundeskriminalamt zum Zoll verlagert.
- Stärkung des risikobasierten Ansatzes.
- Einrichtung eines elektronischen Transparenzregisters.
- Harmonisierung und gleichzeitige Verschärfung der Bußgeldbewehrung von Verstößen gegen geldwäscherechtliche Pflichten.

2020
Weitere umfangreiche Erweiterungen

- Weitere erhebliche Verschärfungen des GwG aufgrund der Umsetzung der Fünften Geldwäscherichtlinie.
- Erweiterung und Konkretisierung des Kreises des Verpflichteten im Finanz- sowie im Nichtfinanzsektor. Nunmehr sollen auch Anbieter von elektronischen Geldbörsen, mit denen virtuelle Währungen (z. B. Kryptos) verwahrt werden, sowie Anbieter von Dienstleistungen für den Wechsel zwischen virtuellen Währungen Verpflichtete sein. Ebenso wurden bestimmte Immobilienmakler und Kunstlagerhalter in den Kreis der Verpflichteten aufgenommen.
- Das Transparenzregister soll weitestgehend für die Öffentlichkeit zugänglich sein.
- Verschärfung der Pflicht zur Verdachtsmeldung für freie Berufe, insb. im Immobiliensektor.

Jüngere Entwicklungen

Durch das Transparenzregister- und Finanzinformationsgesetz soll das Transparenzregister zu einem sogenannten Vollregister werden. Hierdurch wird eine Meldepflicht für wirtschaftlich Berechtigte aller Unternehmen eingeführt, bisherige Mitteilungsfiktionen entfallen.
Inzwischen wurde von der Europäischen Kommission ein neues Regelungspaket entworfen. Dieses besteht aus vier Gesetzgebungsvorschlägen im Bereich der Prävention von Geldwäsche und Terrorismusfinanzierung und verfolgt das übergeordnete Ziel, für Präventionsstandards und die Aufsicht über deren Einhaltung unionsweit einheitliche Standards zu schaffen („Single Rulebook"-Ansatz). Dieses Paket muss noch vom Europäischen Parlament und Rat verabschiedet werden. Fest steht bereits, dass wiederum wichtige Änderungen vorgenommen werden, die sich bedeutend auf Verpflichtete des Finanz- und des Nichtfinanzsektors auswirken werden.

„Zur Vermeidung von Haftungsrisiken müssen sich Unternehmen des Finanz- und des Nichtfinanzsektors stetig vergewissern, dass ihr AML-Risikomanagement die Anforderungen der aktuellen Gesetzeslage und Verwaltungspraxis vollständig und risikoangemessen abbildet."

Charlotte Salathé
Rechtsanwältin, CMS Deutschland

Die richtigen Grundlagen.

Um die Pflichten des GwG erfüllen zu können, müssen Verpflichtete ein funktionsfähiges Risikomanagement implementieren. Ein Risikomanagement besteht typischerweise aus einer Risikoanalyse und daraus abgeleiteten internen Sicherungsmaßnahmen, insb. interner Grundsätze und Verfahren, (falls erforderlich) der Ernennung eines Geldwäschebeauftragten, institutionalisierter KYC-Prüfprozesse und einem Schulungsplan für Mitarbeiter.

1. Festlegung von Verantwortlichkeiten

Benennung eines Verantwortlichen auf Leitungsebene

Verpflichtete müssen zunächst auf Leitungsebene eine für Risikomanagement und Einhaltung geldwäscherechtlicher Bestimmungen verantwortliche Person benennen. In der Regel darf diese Person nicht zeitgleich Geldwäschebeauftragter sein (Ausnahme: sehr kleine Unternehmen).
Der Verantwortliche muss einen vollumfassenden Überblick über das gesamte Risikomanagement haben. Dies wird dadurch sichergestellt, dass er Risikoanalyse und interne Sicherungsmaßnahmen genehmigen muss.

Benennung eines Geldwäschebeauftragten auf Führungsebene

Bestimmte Verpflichteten-Gruppen, insbesondere solche des Finanzsektors, müssen zudem einen Geldwäschebeauftragten auf Führungsebene sowie einen Stellvertreter benennen. Bei Kreditinstituten sind die Geldwäschebeauftragten zugleich „zentrale Stelle“ im Sinne des KWG.
Zu den Aufgaben des Geldwäschebeauftragten zählen insbesondere die folgenden:

- Zuständigkeit für die Implementierung und Überwachung der Einhaltung sämtlicher geldwäscherelevanter Vorschriften im Unternehmen;
- Befassung mit sämtlichen Angelegenheiten zur Prävention von Geldwäsche und Terrorismusfinanzierung im Unternehmen;
- Ansprechpartner für Organe, Mitarbeiter, Aufsichts- und Ermittlungsbehörden sowie die FIU in Fragen zu Geldwäsche- oder Terrorismusfinanzierung;
- Abgabe von Verdachtsmeldungen an die FIU oder Beantwortung von Auskunftsersuchen der FIU oder von Ermittlungsbehörden.

2. Erstellung einer Risikoanalyse und Festlegung von Methoden

Ausgangspunkt eines Risikomanagements ist die Risikoanalyse. Verpflichtete müssen diejenigen Risiken der Geldwäsche und Terrorismusfinanzierung ermitteln und bewerten, die für die von ihnen betriebenen Geschäfte bestehen. Dafür müssen Verpflichtete mindestens Risikofaktoren berücksichtigen, die die folgenden Kategorien abdecken:

- Kundenrisiko
- Produkt-, Dienstleistungs-, Transaktions- oder Vertriebskanalrisiko
- geografisches Risiko
- Ermittlungsbehörden.

Im Finanzsektor hat es sich vielerorts etabliert, die GwG-Risikoanalyse in eine Systematische Integritätsrisikoanalyse (SIRA) einzubetten. Die SIRA-Methode ist umfassender als die reine GwG-Risikoanalyse, indem sie sämtliche Integritätsrisiken abdeckt und damit weitergehenden bankaufsichtsrechtlichen Anforderungen Rechnung trägt.

Stufenplan für eine Risikoanalyse

Um Maßnahmen und Abläufe für das Risikomanagement festzulegen, müssen Verpflichtete zunächst Art und Umfang bestehender Risiken analysieren. Aufbauend auf der Risikoanalyse müssen Verpflichtete interne Grundsätze, Verfahren und Kontrollen in Bezug auf ihre internen Sicherungsmaßnahmen ausarbeiten, die geeignet sind, das individuelle Risiko der Geldwäsche und Terrorismusfinanzierung zu kontrollieren. Der Stufenplan für die Durchführung einer Risikoanalyse sieht folgendermaßen aus:

Schritt 1: Vorbereitung und Bestandsaufnahme

- Führen Sie eine Aufnahme der spezifischen Situation über die Organisation des Geschäftsbereichs / der Zweigstelle / des Tochterunternehmens durch. Untersuchen Sie zu diesem Zweck die Tätigkeiten, Standorte (Länder), Produkte, Transaktionen, Dienstleistungen, Kunden, Vertriebskanäle, Arbeitnehmer und Geschäftspartner (z. B. Lieferanten und Outsourcing-Partner).
- Untersuchen Sie, welche Risiken der Geldwäsche und Terrorismusfinanzierung sich auf welche Weise ergeben können.
- Untersuchen Sie, wie man diese Risiken kontrollieren kann.
- Ermitteln Sie den individuellen „Risikoappetit“ des Unternehmens.

Schritt 2: Risikoerfassung und -identifikation

- Erfassen und identifizieren Sie die unternehmensspezifischen Risikotreiber („Risikodimensionen“), mindestens im Hinblick auf:
  - Kundenbezogene Risiken
  - Produkt-, dienstleistungs-, transaktions- und vertriebskanalbezogene Risiken
  - Geografische Risiken
- Hierfür dienen als Orientierung die Kataloge in Anlage 1 und 2 zum GwG. Beide Kataloge enthalten zu allen vorgenannten Risikokategorien beispielhafte Faktoren und mögliche Anzeichen für ein potenziell geringeres bzw. höheres Risiko. Sie finden die Kataloge beigefügt. Naturgemäß sind nicht alle beispielhaften Faktoren auf jedes Geschäftsmodell anwendbar. Ebenfalls zu berücksichtigen sind das Ergebnis der Ersten Nationalen Risikoanalyse zu Geldwäsche 2018/19 sowie die Leitlinien der EBA zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung. Eventuell gibt es weitere Faktoren, die aus der unternehmensspezifischen Erfahrung heraus Auswirkungen auf das Risikoprofil eines Unternehmens haben könnten.
- Beschreiben Sie die so ermittelte Risikosituation je Risikodimension.

Schritt 3: Risikokategorisierung und -bewertung

- Bewerten Sie die einzelnen Risiken durch Aufteilung in Risikogruppen und gewichten Sie diese nach ihrer Bedeutung. Hierfür müssen Sie eigene Risikostufen festlegen, üblich ist z. B. „gering – mittel – hoch“. Erstellen Sie ggf. (alternativ) Szenarien, also potenzielle Erscheinungsformen der Risiken, und analysieren Sie deren Eintrittswahrscheinlichkeit und potenzielle Auswirkungen.
- Bewerten Sie so das Risikoprofil je Kunde / Geschäftsbeziehung und das Gesamtrisiko („Bruttorisiko“).

Schritt 4: Erfassung interner Sicherungsmaßnahmen

- Erfassen und bewerten Sie nun alle internen Sicherungsmaßnahmen, die derzeit zur Reduzierung des „Bruttorisikos“ implementiert sind. Idealerweise sind die internen

Sicherungsmaßnahmen aus dem „Bruttorisiko“ abzuleiten und dieses weitmöglichst zu reduzieren.

- Interne Sicherungsmaßnahmen sind insbesondere interne Richtlinien, Verfahren und Kontrollen in Bezug auf den Umgang mit Risiken, KYC-Pflichten, ein Verdachtsmeldewesen, die Einhaltung von Aufzeichnungs- und Aufbewahrungspflichten, die Bestellung eines Geldwäschebeauftragten und seines Vertreters, ggf. gruppenweite Verfahren, Zuverlässigkeitsprüfungen und Schulungen für Mitarbeiter (siehe im Detail unten).
- Beschreiben und bewerten Sie die internen Sicherungsmaßnahmen und deren Auswirkungen auf das Bruttorisiko („Nettorisiko“).

Schritt 5: Stetige Überprüfung und Weiterentwicklung

- Schließen Sie etwaige Lücken durch stetige Weiterentwicklung interner Sicherungsmaßnahmen und reduzieren Sie das Risiko der Geldwäsche und der Terrorismusfinanzierung weitmöglichst.

Interne Sicherungsmaßnahmen

Verpflichtete müssen zudem über wirksame Strategien, Abläufe, Verfahren und Kontrollen zur Risikoreduzierung und -steuerung verfügen.

Interne Sicherungsmaßnahmen umfassen insbesondere:

- Die Ausarbeitung interner Grundsätze, Verfahren und Kontrollen.
- Die Bestellung eines Geldwäschebeauftragten.
- Die Schaffung von gruppenweiten Verfahren.
- Die Schaffung und Fortentwicklung geeigneter Maßnahmen zur Verhinderung des Missbrauchs von neuen Produkten und Technologien.
- Die Überprüfung der Mitarbeiter auf ihre Zuverlässigkeit („Know Your Employees“).
- Die erstmalige und laufende Unterrichtung der Mitarbeiter in Bezug auf Typologien und aktuelle Methoden der Geldwäsche und der Terrorismusfinanzierung sowie die insoweit einschlägigen Vorschriften und Pflichten, einschließlich Datenschutzbestimmungen.
- Die Überprüfung dieser Grundsätze und Verfahren durch eine unabhängige Prüfung, soweit diese Überprüfung angesichts der Art und des Umfangs der Geschäftstätigkeit angemessen ist.

Beachten Sie dabei, dass die internen Sicherungsmaßnahmen so implementiert sein müssen, dass sie einer Überprüfung durch die interne Revision, externe Wirtschaftsprüfer und Aufsichtsbehörden zugänglich sind.

3. Erstellen eines Schulungsplans

Verpflichtete müssen ihre Mitarbeiter zum Zwecke eines effektiven Risikomanagements laufend über Typologien und aktuelle Methoden der Geldwäsche unterrichten. Hierdurch sollen die Mitarbeiter lernen, möglicherweise mit Geldwäsche und Terrorismusfinanzierung zusammenhängende Transaktionen zu erkennen und sich in solchen Fällen richtig zu verhalten.

Häufigkeit, Inhalt und Intensität der Schulungen sollten auf die Position der Mitarbeiter zugeschnitten sein.

4. Effiziente Aufzeichnung und Aufbewahrung von KYC-Daten

Die Daten, die im Rahmen der KYC-Prüfung erhoben werden, sind von Verpflichteten aufzuzeichnen und aufzubewahren. Auf diese Weise können Auskunftsersuchen der FIU oder von Ermittlungsbehörden im Hinblick auf bestimmte Kunden oder Transaktionen zuverlässig beantwortet werden. Welche Daten von natürlichen Personen, UBOs, Gesellschaften oder anderen juristischen Einheiten, Trusts oder anderen Rechtsvereinbarungen dokumentiert werden müssen, ist in § 8 GwG festgelegt. Die Daten sind fünf Jahre nach Beendigung der Geschäftsbeziehung oder der Ausführung einer einmaligen Transaktion aufzubewahren, soweit nicht andere gesetzliche Bestimmungen über Aufzeichnungs- und Aufbewahrungspflichten eine längere Frist vorsehen. In jedem Fall sind sie nach Ablauf von zehn Jahren zu vernichten.

Die zehn Schritte der KYC-Prüfung.

Verpflichtete müssen die Identität ihrer Kunden genau kennen, um Risiken einschätzen und beherrschen zu können. Zur Erfüllung der gesetzlichen Vorgaben sollten Verpflichtete folgende zehn Schritte bei der Ausführung der KYC-Prüfung beachten:

In diesem Whitepaper erläutern wir die einzelnen Schritte und veranschaulichen diese anhand von Praxisbeispielen.

1 Identifizieren Sie den Kunden.

Bei der KYC-Prüfung werden die Identität und der Hintergrund des potenziellen Kunden und der relevanten Produkte / Dienstleistungen festgestellt. Der Kunde kann sich mit seinen persönlichen Daten (z. B. mit seinem Namen) identifizieren und angeben. Der Kunde muss dabei angeben, ob er für sich selbst oder als Vertreter für eine juristische Person oder eine andere natürliche Person auftritt.

„Die Erfüllung der Gesetze und Vorschriften bei der Identifizierung ist für Verpflichtete nicht die einzige Herausforderung. Es ist vielleicht sogar noch schwieriger, dafür zu sorgen, dass alles digital und kundenfreundlich abgehandelt wird. Häufig müssen Kunden viele Daten angeben, die sie nicht immer sofort zur Hand haben, beispielsweise die Reisepass- oder Steueridentifikationsnummer. Manchmal müssen sie sich persönlich vor Ort identifizieren. Da die meisten Abläufe mittlerweile digital und „remotely“ erledigt werden, passen diese Identifizierungsanforderungen eigentlich nicht mehr in die heutige Welt. Es gibt Parteien, die auch diesen Teil des Aufnahmeverfahrens digitalisieren können. Das spart nicht nur Zeit, sondern trägt auch zur Kundenzufriedenheit bei. Dadurch erhöht sich wiederum die Wahrscheinlichkeit, dass die Kunden einem lange treu bleiben.“

Daniel Brunzema
Country Manager bei Company.info

2 Überprüfen Sie die Kundenidentität.

Anschließend wird die Kundenidentität überprüft. Dazu müssen häufig offizielle Dokumente zurate gezogen werden.

- Bei natürlichen Personen wird u. a. regelmäßig das amtliche Ausweisdokument (Reisepass, Personalausweis, Führerschein, Reisedokument oder Reisedokument für Ausländer) zur Überprüfung eingesetzt.
- Juristische Personen werden anhand von Informationen aus zuverlässigen und unabhängigen (Daten-)Quellen überprüft. Wenn die juristische Person im Handelsregister eingetragen ist, wird der Auszug aus dem Handelsregister konsultiert.

Der Verpflichtete ist dazu verpflichtet, die Daten und Dokumente, mit denen ein Kunde identifiziert und die Identität überprüft wurde, aufzuzeichnen und aufzubewahren (siehe oben).

3 Stellen Sie fest, ob eine Stellvertretung vorliegt.

Ein Verpflichteter ist im Rahmen der KYC-Prüfung auch dazu verpflichtet, zu kontrollieren, ob der Kunde für sich selbst oder für einen Dritten auftritt. Im Falle einer Stellvertretung müssen sowohl der Stellvertreter als auch der Vertretene identifiziert werden. Zusätzlich muss die Berechtigung der auftretenden Person zur Stellvertretung überprüft werden. Hierdurch soll vermieden werden, dass jemand als „Strohmann“ für einen (kriminellen) Hintermann auftritt.

Um festzustellen, ob ein Kunde in seinem eigenen Namen oder im Namen eines Vertretenen handelt, können Verpflichtete mehrere Indikatoren festlegen, die bei der KYC-Prüfung untersucht werden. Kann die Person beispielsweise bestimmte Fragen über die Größe des Unternehmens, den Standort oder den Ursprung von Geldern nicht beantworten, können dies Hinweise auf ein potenzielles Risiko sein. Liegen tatsächliche Anhaltspunkte dafür vor, dass es sich bei einem Kunden um einen „Strohmann“ handeln könnte, wird dieser – risikoabhängig – einer erhöhten Risikokategorie zugeordnet oder die Geschäftsbeziehung gar nicht erst begründet bzw. beendet.

4 Stellen Sie den Zweck und die beabsichtigte Art der Geschäftsbeziehung fest.

Das GwG sieht vor, dass der Zweck und die beabsichtigte Art der Geschäftsbeziehung festgestellt werden müssen. Anhand dieser Informationen kann der Verpflichtete eventuelle Risiken, die vom Kunden ausgehen, besser einschätzen. Hinweise hierauf ergeben sich meist bereits im Erstgespräch mit dem Kunden. In einigen Fällen ergeben sich Zweck und beabsichtigte Art der Geschäftsbeziehung sogar zweifelsfrei aus der Geschäftsbeziehung. In anderen Fällen können Nachfragen geboten sein, um sich ein vollständiges Bild von Zweck und beabsichtigter Art der Geschäftsbeziehung zu machen.

5 Recherchieren Sie woher das Vermögen und die Ressourcen stammen.

Wenn ein erhöhtes Risiko auf kriminelle Aktivitäten besteht, sind Verpflichtete im Rahmen verstärkter KYC-Pflichten gehalten, mit risikoangemessenen Maßnahmen die Herkunft der im Rahmen einer Geschäftsbeziehung oder Transaktion einzusetzenden Mittel zu bestimmen. Die Informationen sollten möglichst anhand objektiver Dokumente belegt werden, die wie die weiteren KYC-Unterlagen aufgezeichnet und aufbewahrt werden. Neben einer Befragung des Kunden können sich risikoangemessen auch weitere Nachforschungen über Datenbanken bis hin zu On-Site Visits anbieten.

Die Intensität der Nachforschungen müssen Verpflichtete anhand selbst festgelegter Indikatoren bestimmen. Wichtige Anhaltspunkte können dabei sein:

- die Höhe der einzusetzenden Vermögenswerte;
- die Plausibilität der angegebenen Mittelherkunft; oder
- die augenscheinliche Angemessenheit der Mittel in Bezug zu Alter, Beruf und Erscheinungsbild des Kunden.

6 Verschaffen Sie sich Einblicke in die Eigentums- und Kontrollstruktur des Kunden.

Ein Verpflichteter muss auch die Struktur der Unternehmensgruppe untersuchen, der ein Kunde angehört. Das gilt besonders, wenn Zweifel an der Transparenz der Beteiligungsstruktur bestehen. Wenn sich aus der Analyse ergibt, dass die Beteiligungsstruktur komplex ist, Bezüge zu sog. Offshore-Jurisdiktionen bestehen oder keine plausible Erklärung für die Notwendigkeit einer auffällig komplexen Struktur ersichtlich ist, sind dies Anhaltspunkte für die Einordung in eine erhöhte Risikokategorie. Je nach Komplexität der Struktur und deren Plausibilität kann eine Beteiligungsstruktur zur Zuordnung in eine erhöhte Risikokategorie führen und in Ausnahmefällen dazu, dass eine Geschäftsbeziehung nicht begründet oder beendet werden sollte.

Juristische Personen anhand von unabhängigen Datenbanken überprüfen

„Die Überprüfung von Kunden kann sehr zeitaufwändig sein. Der Einsatz intelligenter, unabhängiger Datenbanken kann den Prozess beschleunigen. Datenbanken bieten häufig alle erforderlichen Informationen für die Hintergrundüberprüfung natürlicher und juristischer Personen auf einen Blick.

Dazu gehören beispielsweise Auskünfte über die Beteiligungsstruktur (bis zum Mutterunternehmen), UBO(s), Mitglieder von Verwaltungs- und / oder Aufsichtsorganen, sonstige Zeichnungsberechtigte, Informationen aus Unternehmensdatenbanken, finanzielle Kennzahlen, Jahresabschlüsse, Brancheninformationen, die Anzahl der Mitarbeiter, (negative) Presseberichterstattung, Übereinstimmungen mit PEP-, Sanktions-, Beobachtungs- oder Warnlisten. Diese Informationen können automatisch mithilfe von APIs („Application Programming Interfaces“) in das System zur Kundenannahme aufgenommen werden. Auf diese Weise können die für die KYC-Prüfung zuständigen Mitarbeiter den Kundenannahmeprozess schneller bearbeiten und verfügen immer über präzise und aktuelle Informationen.“

Daniel Brunzema
Country Manager bei Company.info

Ermitteln Sie den UBO

Verpflichtete müssen vermeiden, dass natürliche Personen ihre wahre Identität hinter Gesellschaften oder anderen juristischen Einheiten verbergen, beispielsweise durch den Einsatz von unübersichtlichen juristischen Strukturen. Aus diesem Grund muss der UBO ermittelt werden. Ein UBO ist jede natürliche Person, in deren Eigentum oder unter deren Kontrolle der Kunde letztendlich auf deren Veranlassung eine Transaktion durchgeführt hat bzw. eine Geschäftsbeziehung begründet wird.

Dem GwG zufolge handelt es sich dabei im Allgemeinen um die natürliche Person, die unmittelbar oder mittelbar mehr als 25 % der Kapitalanteile hält oder mehr als 25 % der Stimmrechte kontrolliert oder auf eine vergleichbare Weise Kontrolle ausübt.

Wer im Einzelfall als UBO gilt, ist rechtsformabhängig. Die vorgenannten Schwellenwerte gelten für juristische Personen und sonstige Gesellschaften. Für rechtsfähige Stiftungen und Rechtsgestaltungen, mit denen treuhänderisch Vermögen verwaltet wird, gelten u. a. Treugeber, Verwalter, Stiftungsvorstände oder Begünstigte als UBO, ohne dass es auf Schwellenwerte ankäme. Gesetzliche Vorgaben finden Sie in § 3 Abs. 2 bis 4 GwG. Hilfreich für die Bestimmung des UBO, auch bei mehrstufigen Beteiligungsverhältnissen und in Sonderkonstellationen, sind die FAQ zum Transparenzregister des Bundesverwaltungsamts.

Ernennung eines fiktiven UBO

Wenn auf Grundlage der im GwG vorgegebenen Kriterien kein UBO ermittelt werden kann, muss alternativ ein sogenannter „fiktiver UBO“ benannt werden. Unter fiktivem UBO versteht man natürliche Personen, die gesetzlicher Vertreter, geschäftsführender Gesellschafter oder Partner des Kunden sind. Voraussetzung hierfür ist, dass nach Durchführung umfassender Prüfungen und ohne dass Verdachtsmomente der Geldwäsche oder Terrorismusfinanzierung vorlägen, kein UBO identifiziert werden konnte. Die Prüfmaßnahmen müssen sorgfältig aufgezeichnet und aufbewahrt werden.

Fallbeispiel undurchsichtige Beteiligungsstruktur

„Eine Mandantin von uns, die im Güterhandel tätig ist, unterhält eine langjährige Geschäftsbeziehung zu einem Geschäftspartner in Panama. Bei einer Überprüfung der internen Geldwäscheabteilung war aufgefallen, dass es keine Dokumentation gab, die geeignet war, die als UBO genannten Personen als solche zu bestätigen. Dies identifizierte man zutreffend als risikoerhöhenden Faktor und bat uns um Rat, wie man damit umgehen sollte. Nachdem auch von uns durchgeführte Datenbankrecherchen keine weiterführenden Erkenntnisse zutage förderten, führten wir gemeinsame Gespräche mit Vertretern der Mandantin und dem Geschäftspartner durch. In den Gesprächen ergab sich, dass die UBOs ihre Beteiligungen nicht unmittelbar, sondern über mehrstufige Beteiligungsstrukturen unter Einbeziehung von Trusts und Stiftungen, teilweise auf den British Virgin Islands oder den Cayman Inseln, hielten. Hierbei handelt es sich um sog. Offshore-Jurisdiktionen, die regelmäßig niedrigere Anforderungen an die Transparenz von juristischen Personen stellen. Es gab entsprechend keine Dokumentation, etwa öffentliche Gesellschafterlisten oder Registerauszüge, die eine Stellung als Gesellschafter nachweisen konnte. Auch in Offshore-Jurisdiktionen gilt mittlerweile die Verpflichtung, die UBOs von

„Briefkastengesellschaften“ gegenüber dem Verwalter offenzulegen. Wir baten daher darum, die interne Dokumentation von einem Vertreter des Verwalters unterzeichnen zu lassen und der Mandantin hiervon beglaubigte Kopien zukommen zu lassen. Die UBOs erfüllten diese Bitte unverzüglich. Eine erneute, tiefergehende Hintergrundrecherche förderte keine negative Presseberichterstattung, wie etwa Hinweise auf Steuer- oder Wirtschaftsstraftaten, zutage. Die Geschäftsbeziehung konnte daher fortgesetzt werden, wenngleich wir der Mandantin rieten, den Geschäftspartner aufgrund des Offshore-Bezugs und der komplexen Beteiligungsstruktur einer erhöhten Risikokategorie zuzuordnen und engmaschig wiederkehrenden Überprüfungen, samt Hintergrundrecherchen über Datenbanken, zu unterziehen.“

Charlotte Salathé
Rechtsanwältin, CMS Deutschland

Das Transparenzregister nutzen

Das Transparenzregister wurde in Deutschland mit dem Inkrafttreten des Gesetzes zur Umsetzung der Vierten Geldwäscherichtlinie im Jahr 2017 eingeführt. Mit den zum 1. August 2021 in Kraft getretenen Änderungen des Geldwäschegesetzes (Transparenzregister- und Finanzinformationsgesetz) und dem damit verfolgten Zweck, das Transparenzregister als ein Vollregister zu etablieren, sind die bislang im GwG verankerten Mitteilungsfiktionen ersatzlos weggefallen. Die Folge ist, dass nunmehr – nach Ablauf von Übergangsfristen – alle juristischen Personen des Privatrechts und eingetragenen Personengesellschaften zur Mitteilung an das Transparenzregister verpflichtet sind.

Einige UBO-Daten aus dem Transparenzregister sind der Öffentlichkeit uneingeschränkt zugänglich:

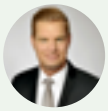
- Vor- und Nachname
- Monat und Jahr der Geburt
- Wohnsitzland
- Art und Umfang des wirtschaftlichen Interesses
- Alle Staatsangehörigkeiten

Das exakte Geburtsdatum und der Wohnort sind nur ausgewählten Behörden oder Verpflichteten zur Erfüllung ihrer eigenen KYC-Pflichten bzw. anderen auf Antrag zugänglich. Für die Überprüfung von UBO-Angaben muss ein Verpflichteter u. a. einen Transparenzregisterauszug einholen.

Unstimmigkeitsmeldungen bei Abweichungen im Transparenzregister

Dass das Transparenzregister ein Hilfsmittel für die KYC-Prüfung darstellt, bedeutet nicht, dass sich Verpflichtete blindlings auf die Informationen im Register verlassen können und dürfen. Bedenken Sie: Die Kunden selbst stellen dem Register die Informationen über die UBOs zur Verfügung. Es besteht daher stets ein gewisses Risiko, dass die Daten falsch oder unvollständig sind. Von den Verpflichteten wird daher erwartet, dass sie auch selbst Untersuchungen im Hinblick auf die UBOs von Kunden durchführen. Wenn einem Verpflichteten auffällt, dass sich die Daten aus dem Transparenzregister von den selbst zusammengetragenen Informationen unterscheiden, müssen die Unstimmigkeiten der registerführenden Stelle gemeldet werden (sog. Unstimmigkeitsmeldung).

„Das Transparenzregister wird mit Ablauf des Jahres 2022 zum Vollregister umfunktioniert sein, sodass alle deutschen juristischen Personen und Personengesellschaften ihre tatsächlichen oder fiktiven wirtschaftlich Berechtigten im Transparenzregister hinterlegt haben. Das Transparenzregister muss bei der Begründung von neuen Geschäftsbeziehungen zwingend in den KYC-Prozess integriert und ein Transparenzregisterauszug eingeholt und dokumentiert werden. Da das Transparenzregister jedoch – anders als das Handelsregister – keinen öffentlichen Glauben besitzt und die Daten ausschließlich von den Kunden eingespeist werden, müssen die Eintragungen im Transparenzregister mit einer gesunden Skepsis betrachtet werden."



Till Komma
Rechtsanwalt, CMS Deutschland

UBOs anhand von unabhängigen Datenquellen überprüfen

Für die eigene Recherche über einen UBO stehen unterschiedliche Anbieter von Unternehmensdatenbanken zur Verfügung. Sie kombinieren Daten aus mehreren Quellen und ermitteln den UBO auf Grundlage der Informationen zur Beteiligungsstruktur und mithilfe von juristischen Dokumenten, wie beispielsweise Handelsregisterauszügen. Einige Datenbanken bieten zuverlässige und exakte Informationen, mit denen Unstimmigkeiten schnell ans Tageslicht kommen. Wenn die Kundeninformationen über den UBO nicht mit den vom Datenlieferanten recherchierten Firmeninformationen übereinstimmen, kann dies als risikoerhöhender Faktor gewertet werden, der weiterer Nachforschungen bedarf.

Situationen, in denen es schwierig ist, den UBO zu verifizieren

1. Die Definition des (fiktiven) UBO ist in jedem Land verschieden

Die Tatsache, dass in jedem Land, auch innerhalb der EU, eine andere Definition für den UBO gilt, erschwert die Ermittlung des UBO oder des fiktiven UBO. Es steht den Mitgliedsstaaten frei, die Definition enger oder weiter zu fassen als es die Richtlinie vorsieht. Deswegen ist oft unklar, wie man als deutscher Verpflichteter einen UBO oder fiktiven UBO im Ausland ermittelt. Beispielsweise, wenn es sich um eine Rechtsform handelt, die dem deutschen Rechtssystem fremd ist. Dafür sind spezifische Kenntnisse erforderlich, die dem Verpflichteten nicht unbedingt zur Verfügung stehen. In diesem Fall kann es sinnvoll sein, externe Fachleute einzuschalten.

2. Mittelbare Beteiligungen bei mehrstufigen Beteiligungsstrukturen

Bei vielen großen Unternehmen gibt es mehrere Beteiligungsebenen und mehrere Beteiligungen auf der gleichen Ebene. Hierbei kann es vorkommen, dass die einzelnen Kapitalanteile und Stimmrechte zwar nicht die relevanten Schwellenwerte überschreiten, um als UBO zu gelten. Allerdings muss beachtet werden, dass die Ausübung von Kontrolle oder eines beherrschenden Einflusses auch durch das Zusammenwirken verschiedener Parallelstränge möglich ist. Teilt sich also eine Beteiligung auf mehrere vertikale Parallelstränge auf, die in einer höheren Ebene wieder in einer natürlichen Person zusammengeführt werden, dann ist diese Person als UBO zu

erfassen. Hierbei handelt es sich häufig um sehr wohlhabende und einflussreiche Personen, die einen bestimmten Prozentsatz ihres Kapitals in verschiedenen Organisationen anlegen, teilweise bewusst unterhalb von UBO- Schwellenwerten. Hierfür kann es unterschiedliche, teils legitime, Gründe geben. Beispielsweise angeführt werden könnte die Angst vor Raub, Erpressung oder Entführung. Gleichzeitig können Schwellenwerte auch bewusst umgangen werden, um den „kriminellen Hintermann“ zu verschleiern. Die Einschätzung solcher Strukturen kann im Einzelfall herausfordernd sein.

3. „Strohmann“-Konstellationen

Teilweise werden „Strohmänner“ oder Nominees eingesetzt, um die Beteiligung der eigentlichen UBOs zu verschleiern. Dabei handelt es sich um Personen, die auf dem Papier Gesellschaftsanteile halten oder anderweitige Berechtigungen aufweisen. Mit den Hintermännern bestehen hierüber Vereinbarungen, meist gegen Entgelt. Solche Konstellationen zu durchschauen, ist in der Praxis häufig schwierig. Ein Indikator für eine „Strohmann“-Konstellation kann sein, dass das äußere Erscheinungsbild des „Strohmannes“ bzw. die in der Öffentlichkeit bekannten Informationen über ihn nicht mit der mutmaßlichen Stellung bei einem Unternehmen übereinstimmen.

Der Fall „Ali Moulaye“ – Milliardenbetrug durch Strohmannkonstellation

Ein Beispiel für eine Strohmannkonstruktion ist der Fall Ali Moulaye. Hier wurde der Name einer Person ohne ihr Wissen benutzt. Der Name und die Unterschrift des belgischen Zahnarztes stehen auf dem Jahresabschluss von insgesamt 385 British Limited (Liability) Partnerships (LLPs / LPs). Dabei handelt es sich um englische Rechtsformen, die ebenso wie eine deutsche Offene Handelsgesellschaft (OHG) mindestens zwei Gesellschafter haben. Allerdings haben sie gleichzeitig eine begrenzte Haftung, wie die deutsche „Gesellschaft mit beschränkter Haftung“ (GmbH). Diese wurden als Briefkastenfirmen betrieben. Solche eignen sich perfekt dafür, den UBO zu verschleiern. Es überrascht daher wenig, dass sich diese Rechtsformen bei Geldwäschern und anderen Wirtschaftskriminellen einiger Beliebtheit erfreuen. Einige dieser LLPs gehörten zum Geldwäschenetzwerk aus Moskau, für das auch die ING Polen Zahlungen leistete. Die LLPs und LPs haben zudem auch eine bedeutende Rolle beim Geldwäscheskandal rund um die estnische Niederlassung der Danske Bank gespielt.

7 Stellen Sie fest, ob es sich beim Kunden oder dem UBO um eine PEP handelt.

Das GwG gibt vor, dass Verpflichtete über Systeme und Abläufe verfügen müssen, um festzustellen, ob der Kunde oder der UBO des Kunden eine PEP ist. Ebenso muss überprüft werden, ob es sich bei dem Kunden oder dem UBO des Kunden um ein Familienmitglied oder eine bekanntermaßen nahestehende Person einer PEP handelt. Wenn dies der Fall ist, muss der Verpflichtete unter anderem mindestens folgende zusätzliche verstärkte KYC-Pflichten durchführen:

- Ein Mitglied der Führungsebene des Verpflichteten muss der Begründung oder Fortführung der Geschäftsbeziehung zustimmen.
- Es sind angemessene Maßnahmen zur Bestimmung der Herkunft der Vermögenswerte, die im Rahmen der Geschäftsbeziehung oder der Transaktion eingesetzt werden, zu ergreifen.
- Die Geschäftsbeziehung ist einer verstärkten kontinuierlichen Überwachung zu unterziehen.

Die PEP muss den Verpflichteten nachvollziehbar über die Herkunft der Vermögenswerte und den Ursprung der Ressourcen informieren, die im Rahmen einer Geschäftsbeziehung oder Transaktion eingesetzt werden.

Als PEP gilt jede Person, die ein hochrangiges wichtiges öffentliches Amt auf internationaler, europäischer oder nationaler Ebene ausübt oder ausgeübt hat oder ein öffentliches Amt unterhalb der nationalen Ebene, dessen politische Bedeutung vergleichbar ist, ausübt oder ausgeübt hat. Eine nicht abschließende Aufzählung, welche Personen insbesondere als PEP zu klassifizieren sind, kann § 1 Abs. 12 Satz 2 Nr. 1 und Nr. 2 GwG entnommen werden.

Wenn ein Kunde oder dessen UBO sein öffentliches Amt nicht mehr ausübt, müssen die verstärkten Sorgfaltspflichten noch so lange wie nötig erfüllt werden. Das GwG sieht hierfür einen Zeitraum von mindestens zwölf Monaten nach Ausscheiden aus dem öffentlichen Amt vor.

8 Führen Sie zu Kunden zu Übereinstimmungen mit Sanktionslisten und negativer Presseberichterstattung durch.

Verpflichtete müssen den Kunden und den UBO auch auf Übereinstimmungen mit anwendbaren Sanktionslisten, insbesondere solchen der EU und Deutschlands, überprüfen. In manchen Fällen kann sich der Abgleich gegen weitere Sanktionslisten anbieten. Zusätzlich sollte eine Hintergrundrecherche nach negativer Presseberichterstattung durchgeführt werden. Auf diese Weise stellt man fest, ob der Kunde oder mit ihm verbundene natürliche oder juristische Personen negativ in der Presse erschienen ist oder ob er bereits mit Terrorismusfinanzierung in Zusammenhang gebracht wurde. Die Durchführung eines solchen Screenings auf negative Medienberichte wird nicht ausdrücklich vorgeschrieben. Sie ist allerdings hilfreich, um festzustellen, welcher Risikokategorie eine Geschäftsbeziehung oder Transaktion zugeordnet werden muss.

9 Führen Sie den Kunden einer Risikokategorie zu.

Die KYC-Prüfung beginnt mit der Erhebung und Überprüfung von Identitätsangaben des Kunden. Die Zuordnung zu einer Risikokategorie ist dabei den Verpflichteten unter Berücksichtigung von Risikofaktoren (Anlagen 1 und 2 zum GwG) weitgehend selbst überlassen. Abhängig von der Risikoklassifizierung wird eine risikoangemessene (vereinfachte, allgemeine oder zusätzlich verstärkte) KYC-Prüfung durchgeführt.

Risikokategorien

In der Praxis hat sich beispielsweise eine dreistufige Risikokategorisierung etabliert:

- Gering
- Mittel
- Hoch

Kunden werden auf Grundlage der Risikoanalyse einer Risikokategorie zugeordnet, die zuvor von dem Verpflichteten definiert wurde (siehe hierzu oben).

- **Kundenrisikofaktoren**
  Situationen mit erhöhtem Risiko sind beispielsweise juristische Personen mit einer undurchsichtigen, komplexen Beteiligungsstruktur sowie Kunden in Branchen, die häufig mit Geldwäsche in Zusammenhang gebracht werden. Dazu zählen unter anderem die Gastronomie, Bordelle, Massagesalons, Immobilienunternehmen und Unternehmen des Glücksspielsektors.

- **Produkt-, Dienstleistungs-, Transaktions- und Lieferkanalrisikofaktoren**
  Wenn der Wert eines Produkts oder einer Dienstleistung schwierig zu ermitteln ist, besteht regelmäßig ein erhöhtes Geldwäscherisiko. Ein gutes Beispiel dafür sind etwa Kunstwerke. Auch der Wert von Immobilien ist häufig schwierig zu ermitteln. Darüber hinaus geht von neuen Technologien teilweise ein höheres Geldwäscherisiko aus. Ein Beispiel hierfür sind Kryptowerte, die, abhängig von ihrer Struktur, zum Teil Anonymität begünstigen (sog. Privacy oder Alt Coins). Auch im Transaktionsverhalten von Kunden kann ein erhöhtes Geldwäscherisiko liegen. Beispiele sind häufig wiederkehrende Transaktionen, die ggf. bewusst unter Schwellenwerten bleiben.

- **Geographische Risikofaktoren**
  Ein erhöhtes Risiko wird Kunden attestiert, die in einem von der FATF oder der EU als Risikoland eingestuften Land niedergelassen sind oder einen Bezug hierzu aufweisen.

Risikokategorie auf Grundlage eines Risikoklassifizierungsformulars festlegen

Um festzulegen, in welche Risikokategorie ein Kunde fällt, kann es sinnvoll sein, ein Risikoklassifizierungsformular auszufüllen. Anhand dieses Formulars können Beziehungs-Produkt-Kombinationen sowie die betreffenden Risikofaktoren untersucht werden.

Risikoklassifizierungsformular (Beispielhaft)

Risikokategorie	Gering	Mittel	Hoch
Länderbasiertes oder geographisches Risiko	0	1	2
Kundenbasiertes Risiko	0	1	2
Produkt-, dienstleistungs- und transaktionsbasiertes Risiko	0	1	2

Risikokategorie	KYC-Prüfung	Risikoscoring	Kommentare
Niedriges Risiko	Vereinfachte KYC-Prüfung	0	Nur im Ausnahmefall
Mittleres Risiko	Allgemeine KYC-Prüfung	1-5	Kein hohes Risikoscoring
Hohes Risiko	Verstärkte KYC-Prüfung	Ab 6	Mit mindestens einem hohen Risikoscoring ggf. Geschäftsbeziehung ablehnen oder beenden.

„Ein häufiger Anwendungsfall vereinfachter Sorgfaltspflichten ist der Rückgriff auf Kopien von Ausweisdokumenten, wenn Geschäftsbeziehungen in Abwesenheit, z. B. online, begründet werden. Verpflichtete sollten darauf achten, vereinfachte Sorgfaltspflichten nur in Ausnahmefällen durchzuführen und genau zu überprüfen, ob die vereinfachten Maßnahmen durch ein tatsächlich geringes Risiko gerechtfertigt sind."

Charlotte Salathé
Rechtsanwältin, CMS Deutschland

Verstärkte KYC-Pflichten

Der Verpflichtete muss nach dem GwG verstärkte Sorgfaltspflichten erfüllen, wenn im Rahmen der Risikoanalyse oder im Einzelfall festgestellt wird, dass ein höheres Risiko der Geldwäsche oder Terrorismusfinanzierung bestehen kann. Ein höheres Risiko kann sich insbesondere aufgrund von Eigenschaften des Kunden oder aufgrund der Art der Transaktion oder Geschäftsbeziehung ergeben. Verstärkte Sorgfaltspflichten müssen auch dann erfüllt werden, wenn der Kunde oder dessen UBO in einem von der Europäischen Kommission als Hochrisikostaat kategorisierten Land lebt oder seinen Unternehmenssitz in diesem Land hat. Das Gesetz legt einige Fälle fest, in denen auf jeden Fall eine verstärkte Sorgfaltspflicht eingehalten werden muss. Das gilt für:

- besonders komplexe und ungewöhnlich große Transaktionen sowie außergewöhnliche Transaktionsmuster, die keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck verfolgen;
- grenzüberschreitende Korrespondenzbeziehungen;
- ein Kunde oder dessen UBO ist oder wird zur PEP oder ist oder wird Familienangehöriger einer PEP oder eine einer PEP bekanntermaßen nahestehende Person.

Neben den oben aufgeführten Fällen kann es noch weitere Gründe für die Einhaltung verstärkter Sorgfaltspflichten geben. Beispielsweise die (körperliche) Abwesenheit bei der Identifizierung. Der Verpflichtete entscheidet selbst, wann die Anwendung verstärkter Sorgfaltspflichten geboten ist und wie er das weitere Vorgehen handhaben möchte. Das heißt, dass der Verpflichtete selbst Indikatoren festlegen kann aber auch muss, die auf ein erhöhtes Risiko hindeuten.

Beispiele für zusätzliche Maßnahmen im Rahmen verstärkter KYC-Prüfung

In § 15 Abs. 4 bis 7 GwG sind einige Maßnahmen aufgeführt, die grundsätzlich im Rahmen der verstärkten Sorgfaltspflichten erfüllt werden müssen.

So muss bei der Beteiligung einer PEP, wie bereits erörtert, vor Begründung oder Fortführung der Geschäftsbeziehung die Zustimmung eines Mitglieds der Führungsebene eingeholt werden. Ebenso muss die Herkunft der Vermögenswerte, welche bei der Geschäftsbeziehung oder Transaktion eingesetzt werden, bestimmt werden. Zudem muss die Geschäftsbeziehung einer verstärkten kontinuierlichen Überwachung unterzogen werden.

Stammt der Kunde oder dessen UBO aus einem Land oder ist in einem Land niedergelassen, das von der Europäischen Kommission als Hochrisikogebiet eingestuft wird, müssen die folgenden verstärkten Sorgfaltspflichten mindestens erfüllt werden:

- Einholen zusätzlicher Informationen über den Vertragspartner und den UBO.
- Einholen zusätzlicher Informationen über die angestrebte Art der Geschäftsbeziehung.
- Einholen zusätzlicher Informationen über die Herkunft der Vermögenswerte und des Vermögens des Vertragspartners über die Herkunft der Vermögenswerte und des Vermögens des UBOs (außer es handelt sich um einen fiktiven UBO).

- Einholen zusätzlicher Informationen über die Gründe für die geplante oder durchgeführte Transaktion.
- Einholen zusätzlicher Informationen über die geplante Verwendung der Vermögenswerte, die im Rahmen der Transaktion oder Geschäftsbeziehung eingesetzt werden, soweit dies zur Beurteilung der Gefahr von Terrorismusfinanzierung erforderlich ist.

Inakzeptable Risiken: keine Geschäftsbeziehungen eingehen oder bestehende Geschäftsbeziehungen beenden

Treten zu viele risikoerhöhende Faktoren zusammen, kann dies dazu führen, dass das Risiko inakzeptabel ist, weil von einem Kunden oder einer Geschäftsbeziehung ein zu hohes Risiko der Geldwäsche oder Terrorismusfinanzierung ausgeht. Der Verpflichtete sollte den Kunden in diesem Fall nicht annehmen oder eine bestehende Geschäftsbeziehung beenden.
Ist ein Verpflichteter nicht in der Lage, die KYC-Prüfung risikoangemessen durchzuführen, so darf eine Geschäftsbeziehung entweder nicht begründet werden oder muss beendet werden. Das kann beispielsweise der Fall sein, wenn nötige Informationen fehlen. Dadurch kann der Verpflichtete die Identität des Kunden nicht zweifelsfrei feststellen und nicht herausfinden, welches (legale) Ziel mit der Geschäftsbeziehung verfolgt werden soll.

Einige Beispiele für inakzeptable Risiken:

- Die Identität des Kunden oder UBO kann nicht überprüft werden (strenge Beendigungspflicht).
- Der Kunde will anonym bleiben oder lediglich fiktive Identitätsangaben machen.
- Der Kunde steht auf einer Sanktionsliste.
- Die vermuteten wirtschaftlichen Verhältnisse eines Kunden stehen in einem extremen Missverhältnis zur bezweckten Art der Geschäftsbeziehung.
- Der Kunde verhält sich unkooperativ, bittet um übermäßige Vertraulichkeit ggf. widerwillig mitgeteilter Informationen.
- Die Organisationsstruktur des Kunden oder der Zweck der Konzernstruktur, der er angehört, erweist sich nach Recherche als auffällig komplex oder ist nicht nachvollziehbar.

10 Überprüfen Sie Kunden in risikoangemessenen Abständen.

Die Risikokategorie, der ein Kunde bei der Annahme zugewiesen wird, ist von großer Bedeutung für die weitere Geschäftsbeziehung. Sie entscheidet darüber, in welchen Abständen der Kunde regelmäßig einer Überprüfung unterzogen wird. Indem Sie Kunden regelmäßig kontrollieren, erfahren Sie, ob die Risikokategorie des Kunden noch zutreffend ist. Im Laufe der Geschäftsbeziehung können sich nämlich die risikobestimmenden Faktoren ändern und die Zuordnung in eine andere Risikokategorie erforderlich machen.

Periodische Aktualisierungen

Bei der periodischen Aktualisierung von KYC-Angaben wird geprüft, ob die Risikokategorisierung eines Kunden noch zutrifft und die angewandten Sicherungsmaßnahmen noch risikoangemessen sind. Dabei werden sämtliche Schritte der KYC-Prüfung, außer der (Erst-)Identifizierung, wiederholt. Welche genauen Maßnahmen im Rahmen der periodischen Aktualisierung erfüllt werden müssen, hängt wiederum von der Risikokategorie ab, der ein Kunde initial zugeordnet wurde. Es ist wichtig, dass der Verpflichtete die Methode zur Risikokategorisierung sowie die Begründung für diese aufzeichnet und ebenso auf Aktualität und Effektivität überprüft.

Der Zeitabstand zwischen Aktualisierungen ist ebenfalls risikoangemessen zu wählen. Risikoangemessen können folgende Zeitabstände sein:

- niedriges Risiko: alle fünf Jahre
- normales Risiko: alle drei Jahre
- hohes Risiko: jedes Jahr

Davon unabhängig muss ein Verpflichteter in der Lage sein, anlassbezogen Ad hoc-Aktualisierungen durchzuführen.

Änderungen des Branchenrisikos sollten ebenfalls berücksichtigt werden.

„Auch die Branchen eines Kunden können sich ändern oder erweitern. Wir spüren diese Änderungen auf, indem wir die Websites von Unternehmen durchsuchen. Auf diese Weise können wir Unternehmen einen zusätzlichen Branchencode zuweisen, der auf den Tätigkeiten basiert, die das Unternehmen auf seiner Website anbietet. In der Praxis trägt diese Information dazu bei, uns zeitnah ein genaueres Bild vom Kunden zu machen."

Daniel Brunzema
Country Manager bei Company.info

Anlassbezogene Aktualisierungen

Neben den periodischen Aktualisierungen kann es vorkommen, dass Kunden auch anlassbezogen überprüft werden müssen. Hier einige Beispiele für Anlässe, die eine anlassbezogene Aktualisierung erforderlich machen:

- Der Kunde hat ein neues Produkt oder eine neue Dienstleistung eingeführt, die eine Veränderung des Risikoprofils zur Folge haben.
- Der Kunde beantragt ein neues Produkt oder eine neue Dienstleistung.
- Es wurde eine außergewöhnliche Transaktion festgestellt.
- Es hat Veränderungen in der Organisationsstruktur gegeben (beispielsweise ein neuer UBO).
- Der Kunde hat den Unternehmenszweck geändert oder wesentlich erweitert (z. B. Erschließung neuer Märkte oder Branchen).
- Es fand ein risikorelevantes Ereignis statt (z. B. vermuteter Betrugsversuch).
- Es gibt negative Presseberichterstattung zu einem Kunden oder einer verbundenen Person.
- Es gibt Zweifel an der Aktualität der Kundendaten.
- Der Kunde selbst meldet Änderungen seiner Stammdaten.
- Die Post an den Kunden ist unzustellbar.

Aus Sicht von Wirtschaftskriminellen ist es erstrebenswert, bei Begründung einer Geschäftsbeziehung einer geringen Risikokategorie zugeordnet zu werden, um möglichst selten einer erneuten KYC-Prüfung unterzogen zu werden und weitmöglich „unter dem Radar“ zu laufen. Verpflichtete sollten daher dennoch verdächtige Verhaltensweisen bei Kunden mit geringem Risiko feststellen können, z. B.:

- Transaktionen, die plötzlich von einem Konto aus getätigt werden, welches lange inaktiv war
- sich wiederholende Transaktionen von kleinen identischen Beträgen in kurzen Zeitabständen
- Änderung der Anschrift in ein „Hochrisiko-Land“
- Beitritt einer PEP als Mitglied des Aufsichts- oder Geschäftsführungsorgans oder UBO

Transaktionsmonitoring und Verdachtsmeldewesen

Auch Transaktionen müssen überwacht werden. Das geschieht nicht in regelmäßigen Zeitabstanden, sondern laufend. Auffällige Transaktionen werden anhand der Transaktionsüberwachung identifiziert. Diese Transaktionsüberwachung verläuft, insbesondere in der Finanzindustrie, regelmäßig automatisch mithilfe von Softwaresystemen. Der Verpflichtete integriert hierzu sog. „Szenarien von außergewöhnlichen, risikoanfälligen Transaktionen“ in dieses System. Sollten dann Transaktionen ausgeführt werden, die einem dieser Szenarien entsprechen, informiert das System den Verpflichteten. Beispielhafte Szenarien sind etwa:

- verhältnismäßig hohe Transaktionsvolumina
- hohe Bargeldtransaktionen
- Transaktionen ins Ausland, insb. in „Hochrisiko-Länder“
- auffällige Namen / Beschreibungen des Verwendungszwecks
- abweichende Muster
- auffällig hoher oder auffällig geringer Transaktionsumfang

Auffällige Transaktionen

Bei auffälligen Transaktionen auf Basis von subjektiven Indikatoren hat der Verpflichtete Veranlassung zu unterstellen, dass die Transaktion mit Geldwäsche oder Terrorismusfinanzierung zusammenhängen kann. Der Verpflichtete, respektive der Geldwäschebeauftragte, beurteilt und schätzt ein, ob die Transaktion der FIU gemeldet werden muss oder nicht.

Nach der Kundenannahme erstellt der Verpflichtete ein Transaktionsprofil für den Kunden. Darin wird vermerkt, welche Aktivitäten und Transaktionen der Verpflichtete vom Kunden erwartet.
Eine Transaktion gilt dann als auffällig, wenn sie nicht dem Zweck und der beabsichtigten Art der Geschäftsbeziehung entspricht. Der Verpflichtete erhält eine Meldung und muss auf dieser Grundlage ein Gespräch mit dem Kunden erwägen. In diesem Gespräch kann sich eine initiale Auffälligkeit z. B. durch nachvollziehbare Erklärungen des Kunden plausibilisieren. Anfängliche Verdachtsmomente können sich durch auffälliges, unkooperatives Verhalten des Kunden allerdings auch erhärten.

Typische Anhaltspunkte für Auffälligkeiten und darauf basierende Meldepflichten sind Übereinstimmungen mit risikoerhöhenden Umständen im Katalog in Anlage 2 des GwG.

Verdachtsmeldepflicht bei auffälligen Transaktionen oder Geschäftsbeziehungen

Liegen Tatsachen vor, die darauf hindeuten, dass

- ein Vermögensgegenstand, der mit einer Geschäftsbeziehung oder einer Transaktion im Zusammenhang steht, aus einer strafbaren Handlung stammt, die eine Vortat der Geldwäsche darstellt;
- ein Geschäftsvorfall, eine Transaktion oder ein Vermögensgegenstand im Zusammenhang mit Terrorismusfinanzierung steht oder
- der Kunde seine Verpflichtung, gegenüber einem Verpflichteten offenzulegen, ob er eine Geschäftsbeziehung für einen abweichenden UBO begründen, fortsetzen oder durchführen will, nicht erfüllt.

so besteht die Pflicht, diese Transaktion an die FIU zu melden (Verdachtsmeldepflicht, § 43 GwG).
Die Meldung muss unverzüglich, d. h. ohne schuldhaften Verzug, abgegeben werden, inhaltlich richtig und vollständig sein.

Eine unterlassene, fehlerhafte oder unvollständige Verdachtsmeldung kann Bußgelder nach sich ziehen.

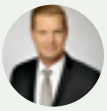
Stillhaltefrist nach Meldung

Transaktionen, wegen denen Verdachtsmeldungen abgegeben worden sind, dürfen frühestens nach dem dritten Werktag nach Abgabe durchgeführt werden, sofern keine abweichende Transaktionsfreigabe oder Transaktionsuntersagung der FIU oder einer Strafverfolgungsbehörde erfolgt.

Tipping Off-Verbot

Der Verpflichtete ist gehalten, über die Beabsichtigung oder die Abgabe einer Verdachtsmeldung Stillschweigen zu bewahren, insbesondere gegenüber dem betroffenen Kunden darf er nicht offenlegen, dass er eine Verdachtsmeldung abgegeben hat. Auf diese Weise soll verhindert werden, dass er gewarnt wird und sich oder seinen Tatertrag dem Zugriff der Strafverfolgungsbehörden entzieht.

„Die Einhaltung des Tipping Off-Verbots kann für Verpflichtete zum Drahtseilakt werden. Denn eine Offenlegung einer Verdachtsmeldung ist nicht nur bei ausdrücklichen, sondern bereits bei stillschweigenden („impliziten“) Hinweisen anzunehmen, die sich zum Beispiel auch aus einem bestimmten Verhalten ergeben können. In praktischer Hinsicht erfordert das für Verpflichtete eine sehr bedachte Verhaltensweise in Geschäftsbeziehungen, in deren Verlauf eine Verdachtsmeldung abgegeben wurde. Es darf nicht der Anschein erweckt werden, dass eine Verdachtsmeldung beabsichtigt oder bereits abgegeben wurde.“



Till Komma
Rechtsanwalt, CMS Deutschland

Die Verdachtsmeldungen sowie dazugehörige Dokumentation müssen aufgezeichnet und mit den KYC-Unterlagen aufbewahrt werden (siehe zur Aufzeichnung und Aufbewahrung oben).

SCHLUSSFOLGERUNG

Der rote Faden: Überwachen Sie Geschäftsbeziehungen sorgfältig und automatisieren Sie Prozesse, wo möglich.

Den Pflichtenkatalog des GwG zu erfüllen, ist zweifellos eine anspruchsvolle Aufgabe, für die es keine „One fits all"-Lösung gibt. Wenn Sie jedoch folgende Keynotes im Hinterkopf behalten, wird Ihnen die Anwendung des GwG etwas leichter fallen.

1. Erstellung einer Risikoanalyse und Festlegung von Methoden

Die Risikoanalyse, die Sie vor der Erstellung einer KYC-Strategie durchführen, dient Ihnen als Grundlage. Sie sollten alles sauber festlegen und dokumentieren. Auf diese Weise können Sie all Ihre Entscheidungen „revisionsfest" belegen. Das gilt nicht nur für die Erstellung einer KYC-Strategie, sondern auch für die Ausführung von risikoangemessenen KYC-Prüfungen. Wenn Sie für die Annahme oder Überwachung von Kunden eine KYC-Prüfung durchführen, geht es darum, Risikoindikatoren zu ermitteln. Dokumentieren Sie alle Schritte, die Sie im Laufe der KYC-Prüfung unternehmen. Auf dieser Grundlage können Sie abwägen, ob Sie bereit sind, die ermittelten Risiken zu akzeptieren oder welche Sicherungsmaßnahmen angewendet werden müssen, um das Risiko zu kontrollieren.

2. Automatisieren Sie die Kundenannahme, wo möglich

Die Durchführung von KYC-Prüfungen verläuft effektiver, wenn Sie die erforderlichen Unternehmensdaten automatisch in Ihr Kundenannahme- oder Überwachungssystem einspeisen. Auf diese Weise werden Risiken frühzeitiger oder schneller erkannt. Dafür können APIs verwendet werden. Damit verfügen Sie umgehend über korrekte, möglichst vollständige und präzise Unternehmensdaten. So sparen Sie viel Zeit: anstatt einzelne Handelsregisterauszüge zu beantragen, haben Sie alle Informationen komplett in Ihrer eigenen Software. Integrieren Sie APIs unter anderem für die Einspeisung von folgenden Unternehmensdaten:

- Organisations- und Kontrollstruktur (bis zum Mutterunternehmen)
- Handelsregisterauszüge

- UBOs
- negative Presseberichterstattung
- Übereinstimmungen mit PEP-, Sanktions-, Beobachtungs- oder Warnlisten
- Informationen über Gerichtsverfahren

3. Stellen Sie Trigger für anlassbezogene Aktualisierungen ein

Natürlich wollen Sie verdächtige Vorgehensweisen oder Veränderungen bei einem Kunden frühzeitig feststellen, um sich zu vergewissern, dass die bisherige Risikokategorisierung noch aktuell ist. Sollten Sie Veränderungen bei einer periodischen Aktualisierung feststellen, kann es bereits zu spät sein. Sorgen Sie also dafür, dass Sie ereignisbasiert über Veränderungen auf dem Laufenden bleiben. Dies gilt besonders bei Kunden, die bei ihrer Annahme einer geringen Risikokategorie zugeordnet wurden. Stellen Sie im Monitoringsystem Alerts für Veränderungen ein, über die Sie in Echtzeit informiert werden wollen.

4. Sorgen Sie dafür, dass Ihre Kenntnisse immer aktuell sind

Last but not least: Sorgen Sie dafür, dass die sachbefassten Mitarbeiter immer über geltende Verpflichtungen und aktuelle Änderungen auf dem Laufenden sind. Erstellen Sie einen Schulungsplan, damit die Einzelheiten des GwG und die einschlägige Verwaltungspraxis genau bekannt sind. Gibt es Änderungen? Untersuchen Sie, ob sich diese auf Ihre Dienstleistungen und die Risiken auswirken. Sollte das der Fall sein, kontrollieren Sie bitte auch, ob Ihre Handbücher und internen Abläufe zur Vermeidung von Geldwäsche und Terrorismusfinanzierung noch aktuell sind. Auf diese Weise verhindern Sie, dass Risiken nicht oder zu spät festgestellt werden und Ihr Unternehmen und die Mitarbeiter nicht in „Haftungsfallen tappen“.

Über Company.info

Company.info setzt Daten in umfassende, übersichtliche und zuverlässige Informationen um und bietet Nachrichten und Prognosen über Unternehmen und ihre Führungskräfte. Auf diese Weise helfen wir Geldwäsche-Compliance-Abteilungen dabei, Risiken schneller einzuschätzen und gut informiert zu entscheiden, ob eine Geschäftsbeziehung eingegangen wird oder nicht. Daten spielen eine bedeutende Rolle bei der Erfüllung des GwG, der Überprüfung neuer Kundenbeziehungen und der Überwachung von bestehenden Kunden. Auf unserem Online-Portal Via finden Sie an einem Ort Einblicke in die Eigentums- und Kontrollstruktur, den UBO, Presseberichterstattung, Jahresabschlüsse und finanzielle Informationen von Unternehmen. Mithilfe der Integration unserer APIs können diese Informationen automatisch in Kundenannahme- und Monitoringsysteme eingespeist werden.

Möchten Sie erfahren, wie wir Sie beim KYC-Onboarding und bei Ihren Monitoringabläufen unterstützen können?
Wir stellen Ihnen gerne unsere Datenlösungen vor.

+49 (0)211 – 540 74 7300
kontakt@company.info