

# Leitfaden Melde- und Sorgfaltspflichten im Gewerbesektor

Wien, Februar 2024



# Einführung

Der Gewerbesektor bietet großes Potential um verdächtiges Verhalten im Bereich der Geldwäscherei und der Terrorismusfinanzierung frühzeitig zu erkennen. Bargeldintensive Geschäfte eignen sich nach wie vor, um inkriminierte Gelder unauffällig in den regulären Wirtschaftskreislauf einzubringen und zu legitimieren. Die Zahl der Verdachtsmeldungen, die die Geldwäschemeldestelle (A-FIU) aus dieser Branche erhält, bewegt sich seit Jahren im niedrigen zweistelligen Bereich. Trotz vergleichbaren Risikos, etwa im Immobiliensektor oder im Edelmetallhandel, verzeichnen andere europäische Financial Intelligence Units sehr viel höhere Meldungszahlen vonseiten der Gewerbetreibenden. Der internationale Vergleich macht den Aufholbedarf und die Notwendigkeit eines erhöhten Bewusstseins für die Risiken Geldwäsche- und der Terrorismusfinanzierung deutlich.

2024 beginnt die mehrjährige und ausführliche Überprüfung des österreichischen Systems zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung durch die Financial Action Task Force (FATF). Ihr Ausgang entscheidet unter anderem über Österreichs (un)eingeschränkte Teilnahme am internationalen Finanzmarkt in den kommenden zehn Jahren. Ein schlechtes Evaluierungsergebnis kann zu einer sogenannten Graulistung führen, was die Teilnahme Österreichs am internationalen Geldverkehr erheblich einschränkt und Studien des Internationalen Währungsfonds bzw. der Weltbank zufolge zu einem Kapitalabfluss von 7 bis 8 % (circa 36 Milliarden Euro) führen könnte. Der wirtschaftliche Gesamtschaden wird für den Fall einer Graulistung Österreichs auf rund 76 Milliarden Euro geschätzt.

Internationale Entwicklungsbanken knüpfen ihre Kreditvergaben regelmäßig an gute Evaluierungsergebnisse der FATF. Ein funktionierendes und entsprechend positiv bewertetes Präventionssystem gegen Geldwäsche und Terrorismusfinanzierung ist meist Grundvoraussetzung für Kreditvergaben bei internationalen Projekten.

Schlechte FATF-Ratings bedeuten für internationale Geldgeber auch erhöhte Sorgfaltspflichten und Sonderprüfungen im Zusammenhang mit österreichischen Kreditnehmern. Für österreichische Unternehmen würde das einen klaren Wettbewerbsnachteil zum Beispiel bei internationalen Förderanträgen bedeuten.

Graulistungen anderer europäischer Staaten in der jüngsten Vergangenheit zeigen, dass auch die Mitgliedschaft in der Europäischen Union und die Einbettung in ein vergleichsweise gut funktionierendes und transparentes westliches Finanzsystem alleine nicht ausreichen, um die strenge Prüfung der FATF zu bestehen.

Dieses Schreiben bildet einen weiteren Baustein im österreichischen Präventionssystem. Es beschreibt Hinweise für Gewerbetreibende, um mögliche Fälle von Geldwäscherei oder Terrorismusfinanzierung früher zu erkennen und gibt Tipps und Tricks im Umgang mit Verdachtsfällen.

# Risikofaktoren im Gewerbesektor

Es gibt zahlreiche Indikatoren, die darauf hinweisen, dass Gewerbetreibende für Zwecke der Geldwäsche oder der Terrorismusfinanzierung missbraucht werden könnten. Die folgende Aufzählung möglicher Indikatoren zur Feststellung von Auffälligkeiten in Bezug auf Geldwäsche oder Terrorismusfinanzierung ist beispielhaft und soll Gewerbetreibenden mögliche Anhaltspunkte für Verdachtsmomente liefern.

- Bestehen auf Barzahlung bzw. ungewöhnliche Bargeschäfte
- Erzeugen von Zeitdruck zum Geschäftsabschluss
- Verweigerung üblicher Auskünfte ohne Angabe von Gründen
- Diskrepanz zwischen agierenden Personen und Geschäft, zB wenn das beabsichtigte Geschäft im Hinblick auf Alter, Kenntnisse etc. nicht zum Kunden passt
- Falsche oder irreführende Angaben des Kunden
- Kunden, die den direkten Kontakt auffällig meiden oder allzu auffällig den Kontakt zu bestimmten Angestellten suchen
- Geschäfte, die aufgrund einer geographischen Distanz zum Wohnsitz des Kunden nicht plausibel erscheinen
- Komplexe Rechtskonstruktionen, deren Eigentums- oder Kontrollverhältnisse nur schwer zu klären und zu verstehen sind
- Geschäfte mit Ländern, die gesellschaftsrechtliche Konstruktionen anbieten, die die Feststellung und Überprüfung der Mittelherkunft erschweren und in denen laut glaubwürdiger Quellen ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht
- Fehlende oder unvollständige Angaben beim Zahlungsauftrag
- Bezahlung mit virtuellen Währungen (speziell, wenn nicht vorab vereinbart und dem Geschäftsmodell nicht entsprechend)
- Vom Kunden bezahlte Auslandsreisen für Geschäftsabschlüsse
- Unübliche bzw. auffällige Geschäftspraktiken in Verbindung mit hohen Beträgen
- Mehrmalige Änderungen der abgesprochenen Vereinbarungen
- Lebensversicherungen: Unplausible Transaktionen (Beitragshöhe und Beweggründe), unregelmäßige Einzahlungen, Bareinzahlungen, auffälligen bzw. unvernünftige Rückkäufe der Lebensversicherung
- Verschleierung von Treuhandbeziehungen oder der wirtschaftlichen Eigentümer bspw. durch Offshore-Konstruktionen
- Zahlung bzw. Lieferung durch unbekannte oder unbeteiligte Dritte
- Mehrmaliges Vertrösten/Ausreden bei der Bereitstellung von Unterlagen.

# Die Meldeplattform goAML

## Allgemeines

goAML ist das Portal der österreichischen Geldwäschemeldestelle, über das meldeverpflichtete Berufsgruppen einfach, strukturiert und hochvertraulich Sachverhalte übermitteln können, wenn sie den Verdacht haben, für Zwecke der Geldwäsche oder der Terrorismus missbraucht zu werden. goAML wurde vom Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) entwickelt und es wird international von zahlreichen FIUs eingesetzt. Die Europäische Union unterstützt Österreich durch den Fonds für die Innere Sicherheit beim Betrieb und der Weiterentwicklung von goAML.



Um goAML nutzen zu können, müssen Sie sich zunächst mit Ihrer ID-Austria (früher: Handy-signatur) beim Unternehmensserviceportal (USP) unter <https://www.usp.gv.at/goaml> anmelden.



**Kofinanziert von der Europäischen Union**

Im USP finden Sie den Link zu goAML auch unter *Themen* → *Steuern & Finanzen* → *Geldwäsche* → *Geldwäschemeldestelle*.

Für die Anmeldung im Meldeportal goAML benötigen Sie goAML-Zugangsdaten. Sollten Sie noch kein goAML-Konto haben, müssen Sie sich erstmalig registrieren (siehe hierzu die erweiterte Anleitung bzgl. Registrierung einer Organisation bzw. einer Person).

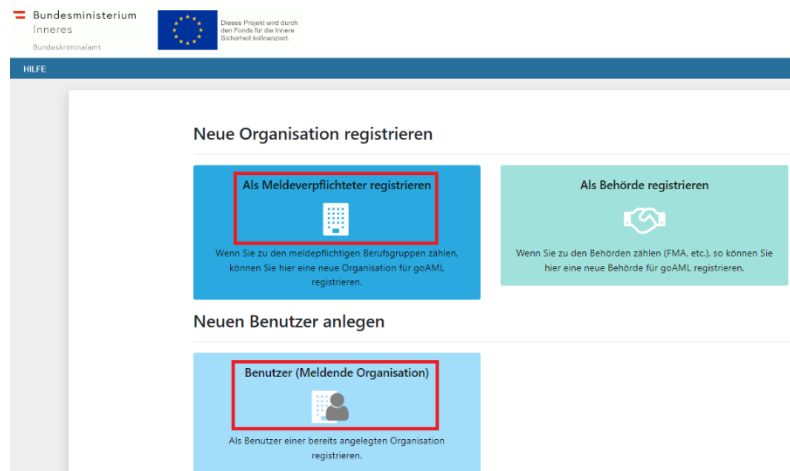
## Registrierung

Die Registrierung bei goAML ist ein einmaliger Vorgang um anschließend Verdachtsmeldungen erstatten zu können.

Sie müssen zunächst ihr Unternehmen als meldeverpflichtete Organisation registrieren.

Ferner haben Sie die Möglichkeit Ihrer einmal angelegten Organisation weitere Benutzer (zB mehrere Compliancearbeitende) hinzuzufügen, die dann selbständig für das Unternehmen bei goAML einsteigen und Verdachtsmeldungen erstatten können.

Administratoren einer verpflichteten Organisation können delegierte Organisationen erstellen, die in deren Namen Meldungen erstatten dürfen.



### Unternehmen registrieren (Anlegen eines Admin-Accounts)

Beim Registrieren einer verpflichteten Organisation wird gleichzeitig auch ein Benutzerkonto für eine Person angelegt. Diese hat automatisch Administratorenrechte für die Organisation. Später können noch weitere Benutzerkonten für die gleiche Organisation angelegt werden.

1. Auf der Hauptseite von goAML links unten auf **REGISTRIEREN** → *Als Meldeverpflichteter registrieren* klicken, um das Registrierungsformular zu öffnen
2. Registrierungsformular ausfüllen:
  - a) rot markierte Felder sind verpflichtend auszufüllen
  - b) E-Mail-Adresse der Organisation wird für Benachrichtigungen an die Organisation verwendet (kann zB ein Funktionspostfach sein)
  - c) für die Erstregistrierung muss eine natürliche Person als Administrator angegeben werden. Daten zur Person (wie zB Benutzername, Passwort) sind personenspezifisch – die Organisation selbst hat kein eigenes Passwort. Als goAML-Administratoren eignen sich insbesondere der/die Geldwäschebeauftragte oder technische Administratoren einer Organisation. Administratoren stehen der A-FIU als Ansprechpartner für technische Rückfragen sowie zur Authentizität der Registrierung zur Verfügung.

- d) Geben Sie im Unterformular unter „Erreichbarkeit(en)“ unbedingt eine Telefonnummer an
3. Antrag absenden (Eine Bestätigung wird an die angegebenen E-Mail-Adressen geschickt)
  4. Die A-FIU prüft anschließend Ihre Registrierung und schaltet Ihr Unternehmen frei (Benachrichtigung darüber erfolgt via E-Mail)

### **Registrieren weiterer Benutzer zu bestehender Organisation**

1. Zu Ihrer bestehenden Organisation können Sie weitere Benutzer (zB mehrere Compliancemitarbeitende) hinzuzufügen, die dann selbständig für das Unternehmen bei goAML einsteigen und Verdachtsmeldungen erstatten können. Dazu muss die goAML-ID-Nummer der Organisation bekannt sein. Diese wurde der erstmaligen Registrierung der Organisation vergeben und kann von jedem Administrator oder Benutzer in den Organisationsdetails eingesehen werden; siehe Details zur Organisation
2. Auf der Hauptseite von goAML links unten auf *REGISTRIEREN* → *Benutzer (Meldende Organisation)* klicken, um das Registrierungsformular zu öffnen
3. Registrierungsformular ausfüllen
  - a) rot markierte Felder sind verpflichtend auszufüllen
  - b) Sie müssen hier keine persönlichen Daten angeben, Pseudonyme und abstrakte Funktionsbezeichnungen (wie zB „Testbank-GWB02“) sind zulässig
4. Antrag absenden (Eine Bestätigung wird an die angegebenen E-Mail-Adressen geschickt)
5. Die Registrierung wird anschließend an den Administrator der Organisation zur Überprüfung und Freischaltung weitergeleitet

### **Administratoren der Organisation**

1. Eingelangte Benutzerregistrierungen können in der Benutzerverwaltung eingesehen werden
2. Sie können die Registrierung nach inhaltlicher Prüfung ablehnen („Zurückweisen“) oder annehmen („Abschließen“). Eine zusätzliche Prüfung durch die A-FIU ist nicht vorgesehen
3. Benutzer werden via E-Mail über die Registrierung oder Ablehnung verständigt

## Registrieren bevollmächtigter Organisationen

Administratoren einer verpflichteten Organisation können delegierte Organisationen erstellen, die Namen der Vollmachtgeberin Meldungen erstatten dürfen. Dazu wählen Administratoren einer bestehenden Organisation im Menü *ADMINISTRATION* → *Organisationsübersicht* die Schaltfläche „*Neue bevollmächtigende Organisation erstellen*“ und tragen im Formular die Daten der zu bevollmächtigenden Organisation ein. Zur delegierten Organisation muss kein Benutzer eingetragen werden. Delegierte Organisationen können dieselbe E-Mail-Adresse verwenden, wie ihre Mutterorganisation.

Sobald die neue Organisation von der A-FIU genehmigt wurde, sehen Administratoren diese in der Organisationsübersicht. In der Hilfe, Kapitel *Bevollmächtigung* wird das Konzept und der Umgang mit bevollmächtigten Organisationen, sowie die Übertragung der Vollmacht genauer beschrieben.

## Verdachtsmeldungen

Meldungen können auf folgende Weise erstattet werden



- Über das Web-Formular (Reiter *NEUE MELDUNGEN* → *Webmeldung erfassen*)
  - mit der Möglichkeit Transaktionsdaten händisch zu erfassen oder mittels Transaktions-XML hochzuladen
- Über reinen XML-Upload
  - Nachteil: bei Zurückstellung nicht wiederverwendbar – kein händisches Verbessern mehr möglich)
- XML-Upload über Web-Formular (seit Version 5.2)
  - händisches kontrollieren und verbessern noch möglich

**Hinweis:** Verdachtsmeldungen an die A-FIU sind ausschließlich über goAML zu erstatten. Hinweise zur Bedienung finden Sie hier: [Registrierung in goAML - Kurzanleitung \(bundeskriminalamt.at\)](#)

## Anonymität der Meldungsleger

Die Wahrung der Anonymität der Verfasser von Verdachtsmeldungen über goAML ist gesichert!

Aufgrund der Sensibilität der übermittelten Daten erfordert die Anmeldung beim Unternehmensserviceportal eine personifizierte Anmeldung, die die vom USP vorgegebene Sicherheitsklasse erfüllt. goAML oder die A-FIU **greifen** auf diese Personeninformationen **nicht zu**. Es ist sichergestellt, dass die personenspezifischen Anmeldedaten der Person (zB Compliance-Officer), die sich am Unternehmensserviceportal authentifiziert hat, nicht an die A-FIU weitergeleitet werden. Die A-FIU **hat keine Möglichkeit**, die beim Unternehmensserviceportal anfallenden Protokolldaten zur Anmeldung auszuwerten.

Eine Authentifizierung der sodann **in goAML** angelegten Nutzer ist nicht notwendig: Bei der Registrierung bzw. Anlage eines Nutzers können Sie auch Pseudonyme verwenden, die die Identität der Nutzer nicht preisgeben. (*Ausnahme*: Technische Administratoren der Organisation).

*Hinweis*: Die Auswertung des USP-Risikoerhebungsbogen erfolgt durch das BMAW bzw durch die Bezirksverwaltungsbehörden.

Bei Problemen mit dem Unternehmensserviceportal steht die **USP-Hotline** von Montag bis Donnerstag von 08:00 bis 16:00 und Freitag von 08:00 bis 14:30 unter **050 233 733**, oder alternativ das [USP-Kontaktformular](#) zur Verfügung.



# Die Sorgfaltspflichten der Gewerbeordnung

Die Gewerbeordnung sieht zahlreiche Bestimmungen zur Prävention von Geldwäscherei und Terrorismusfinanzierung, Sorgfaltspflichten sowie zur verpflichtenden Erstattung von Verdachtsmeldungen und zur Auskunftspflicht gegenüber bestimmten Behörden vor. Die wichtigsten sind hier zusammengefasst.

## Risikobewertung (§ 365n1 GewO)

Eine Risikobewertung ist je nach Größe des Unternehmens und Art der Geschäftstätigkeit unterschiedlich detailliert ausgestaltet und kann aus diversen einzelnen Risiken wie etwa Länderrisiko, Produktrisiko, Transaktionsrisiko oder Kundenrisiko bestehen. Dies dient der Beurteilung des konkreten Risikos anhand geeigneter, unternehmensspezifischer Risikoindikatoren.

- **„Zuständiger Beauftragter“:** Im Zweifel gilt der gewerberechtliche Geschäftsführer Geldwäsche/Compliance-Beauftragte (jedenfalls Führungsebene notwendig)
- **„Angemessene“ Risikobewertung** der konkreten Geschäftstätigkeit entsprechend, ist vorzunehmen, dh individuelle Risiken der Geldwäsche und Terrorismusfinanzierung unter Anwendung diverser Risikofaktoren in Bezug auf Kunden, Länder oder geografische Gebiete, Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle, sind zu ermitteln und zu bewerten sowie nachvollziehbar aufzuzeichnen, auf aktuellem Stand bereit zu halten. Ebenso ist dies der Behörde auf Anfrage in einer verwendbaren Form zur Verfügung zu stellen. Weiters sind Strategien, Kontrollen und Verfahren zur wirksamen Minderung und Steuerung der Risiken von Geldwäsche und Terrorismusfinanzierung zu entwickeln und durch den zuständigen Beauftragten auf Leitungsebene zu überwachen.

## Allgemeine Sorgfaltspflichten (§ 365o GewO)

In bestimmten Situationen wie der Begründung einer Geschäftsbeziehung bestehen allgemeine Sorgfaltspflichten für die Verpflichteten. Folgende Fälle sind hierbei hervorzuheben:

- Begründung einer Geschäftsbeziehung,
- **Abwicklung gelegentlicher Transaktionen in Höhe von 15.000 Euro oder mehr**, und dies unabhängig davon, ob die Transaktion in einem einzigen Vorgang oder in mehreren Vorgängen getätigt wird, wenn zwischen den Transaktionen eine Verbindung zu bestehen scheint,
  - Es gelten hier jedoch noch speziellere Abstufungen je nach konkreter Gewerbeart (Handelsgewerbetreibende - **EUR 10.000 in bar**, etc.)
- **Verdacht auf Geldwäsche oder Terrorismusfinanzierung**, ungeachtet etwaiger Ausnahmeregelungen, Befreiungen oder Schwellenwerte,
- Zweifel an der Echtheit oder der Angemessenheit von Kundenidentifikationsdaten.

## Sorgfaltspflichten gegenüber den Kunden (§ 365p GewO)

Die Kundenidentifizierung und damit das „**Know-your-Customer-Prinzip**“ gilt als eines der wichtigsten Instrumente zur Verhinderung von Geldwäsche und Terrorismusfinanzierung.

- Daher muss der jeweilige Gewerbetreibende über ausreichende Informationen bezüglich der Identität des Kunden verfügen, die wiederum eine notwendige Voraussetzung zur Analyse des Geldwäscherisikos und der sich allenfalls daraus ergebenden weiteren Sorgfaltspflichten, darstellen. In diesem Zusammenhang wird der Vorgang zur Überprüfung der erhobenen Angaben anhand von beweiskräftigen Urkunden und Informationen verstanden. Zweifel an der Echtheit der Dokumente oder Angaben erhöht wiederum das Risiko der Geldwäsche und Terrorismusfinanzierung (siehe Punkt 2).
- Unter den Begriff „**kontinuierlicher Überwachung der Geschäftsbeziehung**“ ist eine aufmerksame Bewertung der Plausibilität der Transaktionen/Abwicklungen zu verstehen und nicht die Überwachung des Kunden an sich.
- Für den Fall, dass **Sorgfaltspflichten nicht eingehalten werden können**, weil sich der Kunde beispielsweise nicht ausweisen will oder keine Angaben zum Zweck des Geschäftes machen will, **muss vom Geschäft abgesehen werden**. Bei Vorliegen eines solchen Falles ist auch eine höhere Wahrscheinlichkeit betreffend Geldwäsche oder Terrorismusfinanzierung anzunehmen und die Vornahme einer Verdachtsmeldung muss in Betracht gezogen werden.

## Identitätsfeststellungen (§ 365q GewO)

Bei Begründung einer Geschäftsbeziehung sowie vor Durchführung einer Einzeltransaktion ist die Identität des Kunden festzustellen.

- Schwellenwert 15.000,00 Euro: Ist der Betrag zu Beginn einer Einzeltransaktion noch nicht bekannt ist, so sind die Feststellungen zu treffen, sobald der Transaktionswert bekannt ist oder sich herausstellt, dass der Schwellenwert erreicht oder überschritten wurde.
- Durchführung vor Begründung einer Geschäftsbeziehung oder Durchführung einer Einzeltransaktion – jedenfalls müssen die Customer Due Diligence-Maßnahmen vor Abschluss eines Vertrages abgeschlossen sein. Vorvertragliche Informationsgespräche sind nicht bereits davon umfasst – es wird jedoch dazu geraten, Informationen einzuholen.
- Die Überprüfung schließt die Identität des Kunden und des wirtschaftlichen Eigentümers mit ein.
- Abs 2: Überprüfung kann erst während der Begründung einer Geschäftsbeziehung abgeschlossen werden, wenn die Nicht-Unterbrechung für einen normalen Geschäftsablauf unbedingt erforderlich ist und nur ein geringes Risiko der Geldwäsche oder der Terrorismusfinanzierung besteht.

## Vereinfachte und verstärkte Sorgfaltspflichten Kunden (§§ 365r, 365s GewO)

Neben der allgemeinen Sorgfaltspflicht gibt es bei Vorliegen bestimmter Umstände vereinfachte sowie bei Kunden oder Sachverhalten mit hohem Risiko erhöhte Sorgfaltspflichten.

- Vereinfachte Sorgfaltspflicht: Eine vereinfachte Sorgfaltspflicht kann angewendet werden, wenn aus der Risikoanalyse lediglich ein geringes Risiko für den Geschäftsfall hervorgeht. Hierbei müssen sich die Verpflichteten jedoch vergewissern, dass die Geschäftsbeziehung oder die Transaktion tatsächlich bloß mit geringem Risiko verbunden ist. Eine Überwachung der Transaktion bzw. der Geschäftsbeziehung ist nichtsdestotrotz durchzuführen. Vereinfachte Sorgfaltspflichten in diesem Zusammenhang gelten vor allem für die Feststellung und Überprüfung der Kundenidentität, der Identität des wirtschaftlichen Eigentümers, die Bewertung und gegebenenfalls Einholung von Informationen über den Zweck und die angestrebte Art der Geschäftsbeziehung, die kontinuierliche Überwachung der Geschäftsbeziehung.

- Verstärkte Sorgfaltspflicht: Ebenso besteht unter Vorliegen bestimmter Umstände die Pflicht verstärkte Sorgfaltspflichten anzuwenden. Die verstärkte Sorgfalt gilt unter anderem gegenüber dem Kunden oder wirtschaftliche Eigentümer, wenn es sich dabei um PEP (Politisch exponierte Personen) handelt oder zu einer solchen ein Naheverhältnis besteht; bei Vorliegen eines Drittlandes mit erhöhtem Risiko (Kunde oder dessen wirtschaftlicher Eigentümer); die Risikobewertung des Kunden bzw. des Geschäfts ergibt ein hohes Risiko; es liegen besonders komplexe bzw. große Transaktionen vor, die ungewöhnlich ablaufen oder deren wirtschaftlicher oder rechtmäßiger Zweck lässt sich nicht nachvollziehen. Die verstärkten Sorgfaltspflichten bestehen zusätzlich zur allgemeinen Sorgfaltspflicht und umfasst Maßnahmen je nach dem vorliegenden risikoerhöhenden Umstand, beispielsweise eine erhöhte Überwachungspflicht.

### Allgemeine Meldepflichten (§ 365t GewO)

Entsteht bei den meldepflichtigen Berufsgruppen der berechtigte Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäscherei oder mit Terrorismusfinanzierung steht, sind sie zur Erstattung einer Verdachtsmeldung an die A-FIU verpflichtet.

- Abgabe einer Verdachtsmeldung bei Kenntnis, Verdacht oder berechtigten Grund zur Annahme:
  - Transaktion (alle Transaktionen, auch versuchte) im Zusammenhang mit Vermögensbestandteilen steht, die aus einer relevanten Straftat (§ 165 StGB) stammt,
  - Vermögensbestandteil aus einer relevanten strafbaren Handlung herrührt,
  - Transaktion oder Vermögensbestandteil iZm Terrorismusfinanzierung steht.
- Unabhängig von der Höhe der Transaktion, Schwellenwerte gelten hier nicht!
- Geringe Schwelle zur Vornahme einer Meldung (bereits berechtigter Grund zur Annahme) – es muss nicht die konkrete Straftat bekannt sein.
- Zusammenarbeit mit der A-FIU in vollem Umfang, Gewerbetreibende haben der Geldwäschemeldestelle auf Verlangen unmittelbar alle erforderlichen Auskünfte zur Verfügung zu stellen und das unabhängig von einer etwaigen zuvor erstatteten Verdachtsmeldung

## Unterlassen der Transaktion (§ 365u GewO)

- Nachdem die Gewerbetreibenden eine Verdachtsmeldung an die A-FIU erstattet haben, haben sie von der Durchführung des Geschäft Abstand nehmen und alle weiteren besonderen Anweisungen der Geldwäschemeldestelle zu befolgen.
- Die A-FIU kann laufende oder bevorstehende verdächtige Transaktionen per Anordnung untersagen.
- Werden von den Gewerbetreibenden Informationen im guten Glauben an die A-FIU weitergegeben, gilt dies nicht als Verletzung einer vertraglichen oder in einer Rechts- bzw. Verwaltungsvorschrift geregelten Beschränkung zur Informationsweitergabe. Die in diesem Fall anzuwendende Geldwäschebestimmung umfasst die Weitergabe.

## Verbot der Weitergabe von Informationen (§ 365w GewO)

Neben der unverzüglichen Meldung an die A-FIU besteht für die Gewerbetreibenden zudem die Pflicht die erstattete Verdachtsmeldung gegenüber den Betroffenen geheim zu halten. Dies gilt auch gegenüber Dritten. Das Verbot gilt nicht gegenüber den zuständigen Behörden bzw. bei Weitergabe zu Zwecken der Strafverfolgung.

## Datenschutz, Aufbewahrung, Statistik (§ 365y GewO)

- Bestimmte Dokumente/Informationen müssen vom Gewerbetreibenden für mindestens 5 Jahre nach Durchführung der letzten Transaktion oder Beendigung der Geschäftsbeziehung aufbewahrt werden und müssen so aufbewahrt werden, dass sie im Falle eines Auskunftersuchens der A-FIU rasch übermittelt werden können. Hierbei gemeint sind vor allem folgende Unterlagen:
  - Unterlagen und Angaben, die der Identifizierung von Kunden dienen (Ausweisdokumente)
  - sämtliche Belege und Aufzeichnungen im Zusammenhang mit Geschäftsbeziehungen und Transaktionen
  - Für Versicherungsvermittler bestehen wiederum spezielle Pflichten

# Informationen durch die A-FIU

Die A-FIU ist verpflichtet den Meldeverpflichteten Informationen über aktuelle Methoden und Phänomene der Geldwäscherei und Terrorismusfinanzierung zur Verfügung zu stellen. Die vermittelten Informationen bieten eine Hilfestellung für die praktische Prüfung von Sachverhalten. Die A-FIU stellt diese Informationen in Form von speziellen Mitteilungen (farblich kategorisiert) auf goAML zur Verfügung.

Die A-FIU empfiehlt daher sich bei goAML zu registrieren, um die relevanten Informationen zu erhalten und für die Risikoanalyse zu nutzen. Zudem gibt die A-FIU zu jeder eingelangten Verdachtsmeldung und deren Status automationsunterstützt Rückmeldung.

Die Mitteilungen sind nach Zweck farblich kategorisiert:

## **Red Notice – Warnmitteilung**

Dringliche Warnung zu einem konkreten und aktuellen Modus Operandi; enthält personenbezogene Daten und Informationen, die für die Implementierung in das Transaktionsmonitoring besonders geeignet sind; rasches Handeln der Meldeverpflichteten unbedingt erforderlich.

Aufgrund ihrer Sensibilität werden Red Notices ausschließlich den betroffenen Berufsgruppen über das persönliche goAML-Messageboard zugestellt. Sie werden per E-Mail verständigt, wenn eine neue Red Notice im goAML-Messageboard verfügbar ist.

## **Purple Notice – Phänomene, Trends & Muster**

Informationen über festgestellte Phänomene, Trends und Muster, die über den konkreten Einzelfall hinausgehen; kann auch Informationen enthalten, die aus behördenübergreifender Zusammenarbeit resultieren; bietet Input im Kampf gegen Geldwäscherei und Terrorismusfinanzierung und kann von den Meldeverpflichteten nach eigener Beurteilung eingesetzt werden. Purple Notices werden auf der goAML Homepage zur Verfügung gestellt.

## **Green Notice – Neuigkeiten aus der A-FIU**

Allgemeine Informationen der A-FIU, die kein Handeln der Meldeverpflichteten erfordern; dient bspw. der Information über weitere Entwicklungen zu bekannten Fällen, Zwischenständen oder Erfolgen vorangegangener Warnmitteilungen; generelle Informationen zur goAML, Meldungserstattung und sonstigen Entwicklungen.

Green Notices werden auf der goAML Homepage zur Verfügung gestellt.

**A-FIU im Bundeskriminalamt**

Josef-Holaubek-Platz 1, 1090 Wien

[www.bundeskriminalamt.at/a-fiu](http://www.bundeskriminalamt.at/a-fiu)