



goAML: Frequently Asked Questions (FAQ)

Stand: Oktober 2024

Version: 5.2

Allgemeine Fragen

1	Wie werden der MROS Verdachtsmeldungen und sonstige Informationen übermittelt?	Seit dem 1. Januar 2020 werden der MROS Verdachtsmeldungen sowie weitere Informationen ausschliesslich über das Datenverarbeitungssystem goAML eingereicht.
2	Wo findet man weiterführende Informationen zum Datenverarbeitungssystem goAML?	Weiterführende Informationen zu goAML werden regelmässig auf folgender MROS-Internet-Seite publiziert: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html Systembezogene Informationen können auch auf der Internet-Seite der UNODC abgerufen werden: https://goaml.unodc.org/. Die auf dieser Seite publizierten Informationen sind jedoch genereller Natur und gehen nicht auf die landespezifischen Anpassungen durch die MROS ein. Hierfür verweisen wir auf die Internetseite der MROS.
3	Muss sich ein Finanzintermediär unter allen Umständen in goAML registrieren lassen?	Eine grundsätzliche Registrierungspflicht in goAML existiert nicht. MROS empfiehlt den meldepflichtigen Finanzintermediären, sich erst dann für die Benutzung von goAML registrieren zu lassen, wenn sie eine Verdachtsmeldung oder eine Antwort auf eine Art. 11a-Anfrage seitens MROS erstatten möchten bzw. müssen.

Anmeldung goAML

4	Weshalb wurde für die Nutzung von goAML eine Zwei-Faktor-Authentifizierung eingeführt?	Um den bereits hohen Sicherheitsstandard zu verbessern, hat MROS für die Systemanmeldung von externen Benutzern von goAML zusätzlich eine Zwei-Faktor-Authentifizierung eingeführt. Die entsprechende Registrierungsseite ist im Internet unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung/registrierung.html aufgeschaltet.
---	---	--



		Auf unserer Homepage steht zum Registrierungsablauf eine detaillierte Schritt-für-Schritt Anleitung zur Verfügung.
5	Kann ich mein goAML-Passwort selber ändern?	Nein, da das Passwort in einem separaten System gespeichert wird, benötigen wir immer eine schriftliche Anfrage an goaml.info@fedpol.admin.ch . Zwingend anzugeben ist dabei die LoginID.
6	Ich habe das Passwort eingegeben und konnte mich nicht einloggen. Was soll ich machen?	Löschen Sie zuerst die History (Cache) Ihres Browsers und starten Sie ihn neu. Sollte das Login trotz Eingabe des korrekten Passwortes nicht klappen, kontaktieren Sie uns bitte via goaml.info@fedpol.admin.ch und wir stellen Ihnen ein Temporär-Passwort zu.
7	Ich habe mich seit langem nicht mehr in goAML angemeldet und mein Login-Versuch war nun erfolglos.	Die Einstellungen im Sicherheitsportal (SSO) sind so gewählt, dass ein Account sechs Monate nach dem letzten erfolgreichen Login deaktiviert wird. Bitte kontaktieren Sie die MROS via goaml.info@fedpol.admin.ch und Ihr Account wird entsperrt.
8	Ich bin als goAML-Admin registriert. Kann ich für meine Kollegen neue Accounts erstellen?	Nein, aufgrund der 2-Faktor-Authentifizierung ist dies nicht möglich. Alle neuen Benutzer müssen demnach das auf unserer Internetseite publizierte Antragsformular ausfüllen: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung/registrierung.html . Sobald sich die neue Person jedoch im goAML registriert hat, ist es die Aufgabe des goAML-Administrators, die Registrierungsanfrage zu überprüfen und freizugeben (finalisieren).

Technische Anforderungen und Datensicherheit

9	Was bedeutet „XML“?	„XML“ ist eine IT-Sprache, welche dazu dient, grosse Datenmengen (z.B. einer Verdachtsmeldung) zu strukturieren.
10	Welche technischen Anforderungen müssen erfüllt sein, um goAML von Seiten der Finanzintermediäre nutzen zu können?	Im Falle eines manuellen Meldevorgangs reichen ein Internetzugang sowie die persönlichen Login-Daten, um sich ins Web-basierte Erfassungstool einzuloggen. Voraussetzung hierfür ist eine vorgängige Registrierung als Benutzer von goAML. Bei der halb- (siehe Frage 27) resp. automatisierten Meldungserstellung wird vorausgesetzt, dass der Finanzintermediär eine interne IT-Lösung entwickelt hat, die dafür sorgt, dass die XML-Datei in der durch die MROS definierten Struktur erstellt wird (die Struktur ist im Internet im Dokument „ <i>Standard XML Reporting – Instructions and Specifications for goAML</i> “ publiziert: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html).



11	Welche Webbrowser werden von goAML unterstützt?	Zurzeit werden die Browser Mozilla Firefox, Google Chrome und Microsoft Edge (Chromium; nur ab 2020 Version) für die Benutzung von goAML unterstützt. Der Webbrowser Internet Explorer IE und ältere Edge-Versionen können nicht verwendet werden.
12	Wie sicher sind die Daten, welche im neuen Datenverarbeitungssystem gespeichert sind?	Die eingereichten Daten gelangen via sichere HTTPS-Verbindung vom Finanzintermediär in die „Demilitarisierte Zone“ (DMZ). Die DMZ befindet sich ausserhalb des Bundes-Netzwerks und wird durch Firewalls, verschlüsselte Kommunikation, Antiviren-Software und Benutzeridentifikation via Zwei-Faktoren-Authentifizierung geschützt. In regelmässigen, kurzen Zeitabständen werden die fertigen Meldungen von der DMZ via einseitigen „Daten-Hol-Mechanismus (Pull)“ ins Bundesnetzwerk übertragen und in der DMZ gelöscht. Im Bundesnetzwerk werden die Daten durch erweiterte IT-Sicherheitsmassnahmen streng geschützt.
13	Werden persönliche Daten der goAML-Benutzer an Dritte weitergeleitet?	Nein. Zu keinem Zeitpunkt werden persönliche Angaben der registrierten goAML-Benutzer an jegliche Dritte weitergegeben. Bei der Übermittlung einer Verdachtsmeldung seitens MROS an eine Strafverfolgungsbehörde werden die Angaben der meldenden Compliance-Mitarbeitenden nicht ersichtlich sein.
14	Kann die UNODC auf die Daten von MROS greifen?	Nein, dies ist niemals der Fall. UNODC ist lediglich der Software-Anbieter, darf jedoch von Gesetzes wegen zu keinem Zeitpunkt in die Daten von MROS Einsicht haben oder darauf zugreifen.
15	Ist es möglich, eine bereits archivierte Meldung anzuschauen resp. herunterzuladen?	Nein, wenn eine Meldung als «archiviert» angezeigt wird, gibt es keine Möglichkeit, diese nochmals anzuschauen resp. herunterzuladen. Es ist deshalb wichtig, dass jeweils sofort nach dem Absenden einer Meldung eine lokale Kopie gespeichert wird.
16	Ich habe irrtümlich einen falschen Reporttyp ausgewählt und die Meldung wurde in der Folge von der MROS zurückgewiesen. Muss ich alles nochmals erfassen?	Nein, sofern die Neubearbeitung des Reports zeitnah geschieht, also der Report noch nicht archiviert ist, kann dieser rückgängig gemacht werden. Der Report befindet sich anschliessend im Ordner «Entwürfe». Ein Klick auf den Reporttyp (oben links in der Maske) öffnet ein Untermenü, wo ein anderer Reporttyp ausgewählt werden kann. Aus einem AIF kann so z.B. ein SAR oder ein CANCL erstellt werden und aus einem AIFT ein STR oder CANCT. Dies ist auch in gegengesetzter Richtung möglich (STR zu AIFT/CANCT, SAR zu AIF/CANCL).
17	Ich bekomme die automatisierten goAML-Benachrichtigungen nicht, obwohl ich eine neue Nachricht im Message-Board habe.	Bitte überprüfen Sie Ihre Einstellungen. Oft sind firmeninterne Sicherheits-Vorkehrungen der Grund dafür, dass solche automatisierten Benachrichtigungen vom Absender «goAML Workflow [mailto:goamIVALIDATION@fedpol.admin.ch] » geblockt werden.



18	Warum kann ich eine erstattete Meldung resp. eine Message Board-Nachricht nicht mehr anschauen resp. für meine Unterlagen speichern?	Aus Sicherheits- und Speicherkapazitätsgründen werden Meldungen und Message-Board-Mitteilungen samt Beilagen nach einer gewissen Zeitspanne vom System automatisch gelöscht. Die Löschrufen sind wie folgt: Übermittelte Meldungen: 7 Tage nach Übermittlung Zurückgewiesene Meldungen, die bereits in den Entwurf-Status verschoben wurden: 7 Tage Meldungsentwürfe: 14 Tage Message Board Nachrichten: 30 Tage
----	---	--

Meldevorgang

19	Wie sieht der Prozess zur manuellen Erfassung einer Meldung in goAML aus und wie gross ist der zeitliche Aufwand?	Die manuelle Datenerfassung (sei dies im Zusammenhang mit einer Verdachtsmeldung oder aufgrund einer Aufforderung zur Herausgabe von Informationen i.S. von Art. 11a Abs. 1 und 2 resp. 3 GwG) kann via Internet direkt durch die im System als User registrierte Personen am Bildschirm erfolgen. Dazu sind die relevanten Angaben online einzugeben und die einzelnen Felder auszufüllen. Je nach Art der Meldung kann die manuelle Erfassung zeitaufwändig sein. Insbesondere, wenn viele Transaktionen zu erfassen sind. Die Erfassung erfolgt ohne den Einsatz weiterer Dritt-Systeme vollständig online. Informationen zu den weiteren Erfassungsmöglichkeiten können im Internet unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html gefunden werden.
20	Müssen alle Transaktionen elektronisch eingereicht werden?	Es sollen alle verdächtigen Transaktionen (bis max. 100 Transaktionen) in elektronischer Form eingereicht werden. Dies bedeutet, dass sie entweder vollständig manuell oder halbautomatisiert (siehe Frage 27) in goAML zu erfassen sind oder mittels XML-Datei übermittelt werden können. Bitte konsultieren Sie hierzu auch unser Dokument «new-fact-sheet-web-reports (hier unter dem Reiter <i>Dokumente</i> zu finden).
21	Reicht es, wenn nur die verdächtigen Transaktionen gemeldet werden oder müssen alle Transaktionen, welche in eine bestimmte Zeitperiode fallen, eingereicht werden?	Ja, es werden lediglich die verdächtigen Transaktionen verlangt (bis max. 100 Transaktionen). Im Meldetext muss explizit begründet werden, wieso der Finanzintermediär weiss oder den Verdacht hat, dass die involvierten Vermögenswerte inkriminiert bzw. verbrecherischen Ursprungs sind. Die MROS kann zur Vervollständigung der erhaltenen Meldung jederzeit von ihrem Recht gemäss Art. 11a Abs. 1 GwG Gebrauch machen und vom meldenden Finanzintermediär



		nachträglich zusätzliche Angaben u.a. zu Transaktionen einfordern. Diese Transaktionen sind der MROS ebenfalls via goAML einzureichen.
22	Gilt die Grenze von max. 100 gemeldeten Transaktionen auch für Reports des Typs AIFT?	Nein, diese Grenze gilt explizit nicht für AIFT-Reports. Antwortet ein Finanzintermediär beispielsweise mittels AIFT auf eine Aufforderung seitens MROS zur Herausgabe von Informationen i.S. von Art. 11a Abs. 1 oder 2 GwG, so kann er pro einzelnen AIFT-Report bis zu max. 1'000 Transaktionen melden. Sind mehr als 1'000 Transaktionen involviert bzw. zu melden, können weitere AIFTs mit jeweils max. 1'000 Transaktionen erfasst und übermittelt werden.
23	Welche Informationen müssen als Beilage eingereicht werden?	Gemäss Art. 3 MGwV sind zwingend erforderliche Dokumente, wie z.B. Passkopien und Kontoeröffnungsunterlagen, als Beilage einzureichen.
24	In welchen Formaten können Beilagen eingereicht werden?	Die akzeptierten Formate sind *.zip; *.xml; *.txt; *.tif; *.tiff; *.bmp; *.doc; *.docx; *.pdf; *.jpg; *.xls; *.xlsx; *.ppt; *.pptx; *.png; *.rtf; *.anb. Die Benutzer werden gebeten, immer die optische Texterkennung OCR (Optical Character Recognition) anzuwenden. Die maximale Grösse pro Attachment ist 20 MB.
25	Wie sieht der Prozess zur Einreichung einer Verdachtsmeldung via XML-Datei aus?	Die automatisierte Meldungserstellung setzt voraus, dass der Finanzintermediär eine interne IT-Applikation programmiert hat, die dafür sorgt, dass die XML-Datei in der durch MROS definierten Struktur erstellt wird. Die Struktur der XML-Datei ist auf der Internetseite der MROS im Dokument "<i>Standard XML Reporting – Instructions and Specifications for goAML</i>" publiziert: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html. Hierzu müssen die nötigen Informationen aus den internen Systemen des Finanzintermediärs abgerufen und anschliessend in der definierten XML-Struktur zusammengestellt werden. Die Bereitstellung der dafür notwendigen IT-Lösung liegt in der Verantwortung des jeweiligen Finanzintermediärs. Wird für die Meldungserstellung der oben beschriebene automatisierte Meldevorgang gewählt, kann anstelle der reinen XML-Datei auch ein ZIP-File übermittelt werden, das neben der XML-Datei alle einzureichenden Beilagen (z.B. Eröffnungsunterlagen, Passkopie, Unterschriftenkarte etc.) enthält.
26	Gibt es eine Mindestanzahl an Meldungen pro Jahr, ab welcher sich die Implementierung einer IT-Lösung zur Erstellung einer XML-Datei definitiv lohnt?	Es kann keine Mindestanzahl definiert werden, da dies nicht nur von der Anzahl der Meldungen abhängt, sondern auch davon, wie umfangreich die einzelnen Meldungen sind. Theoretisch könnte es sein, dass eine Bank im Durchschnitt jährlich nur eine Meldung einreicht, diese dann aber so umfangreich ist, dass die Bank den manuellen Aufwand nicht erbringen möchte und sich für



		die Implementierung einer IT-Lösung zur Erstellung einer XML-Datei entscheidet. Auch zusätzliche Informationen, welche der MROS nach Art. 11a Abs. 1 und 2 GwG zu übermitteln sind, bedürfen einer Erfassung im System. Transaktionsdetails sind auch in diesen Fällen elektronisch und nicht als Beilagen einzureichen.
27	Ist die automatisierte Erstellung einer XML-Datei zwingend nötig?	Die automatisierte Report-Erstellung via XML-Upload kann, muss aber nicht zwingend implementiert werden. Falls die Erstellung einer XML-Datei in automatisierter Form in Betracht gezogen wird, kann diese jederzeit von den meldepflichtigen Instituten eingeführt werden.
28	Gibt es eine Mischform zwischen manueller und automatisierter Meldungseinreichung?	Es ist möglich, eine halbautomatisierte Erfassung der erforderlichen Daten vorzunehmen und die Transaktionen via einem XML-File in die Verdachtsmeldung zu integrieren. Fehlende Daten (rot markierte Felder; z.B. Nationalität des Vertragspartners) können anschliessend manuell ergänzt werden, wobei gleiche Informationen nur einmal und nicht pro Transaktion ergänzt werden müssen. Diese Funktionalität führt zu Zeitersparnissen für diejenigen Finanzintermediäre, welche die automatisierte Lösung nicht umsetzen möchten, jedoch eine grössere Anzahl von Transaktionen zu melden haben und diese ansonsten vollständig manuell erfassen müssten. Damit diese Option genutzt werden kann, müssen die Transaktionen aus dem Bankensystem in strukturierter und vordefinierter Form als XML-Datei gespeichert werden. Unter dem nachfolgenden Link finden Sie im Reiter <i>Dokumente</i> zusätzliche Informationen zum Thema Transactions-Upload: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html
29	Wieso besteht die MROS auf die vollständig elektronische Einreichung der Verdachtsmeldungen?	Die elektronische Datenverfügbarkeit erlaubt es der MROS, weitreichende Analysemöglichkeiten anzuwenden, indem grosse Datenmengen effizient und effektiv beurteilt werden können. Die Daten können automatisiert verlinkt werden, Zusammenhänge werden schneller erkannt und durch das System z.B. als Grafik aufbereitet.
30	Wie soll ich IBAN-Nummern erfassen?	Es wird bevorzugt, dass IBAN-Nummern am Stück also ohne Leerzeichen erfasst werden. Dies erleichtert nicht nur die spätere Suche, sondern verbessert auch die Datenqualität des Systems.
31	Wie muss ich als kontoführendes Bankinstitut vorgehen, wenn ich den Abbruch einer Geschäftsbeziehung	Abbruchsmittelungen gemäss Art. 9b GwG können via spezifischem Reporttyp (CANCL bzw. CANCT), ebenfalls im Webportal goAML unter dem Menü «Neue Meldungen» (Anleitungen siehe hier), erfasst und gemeldet werden.



	i.S. von Art. 9b GwG melden muss?	
32	Erhalte ich nach der Übermittlung einer Abbruchmitteilung i.S. von Art. 9b GwG seitens MROS ebenfalls eine definitive Empfangsbestätigung?	Nein, der meldende Finanzintermediär erhält seitens MROS bei Abbruchmitteilungen keine definitive Empfangsbestätigung. Die im goAML-Webportal verzeichneten Übermittlungsdaten (Message Board-Benachrichtigung -> siehe Screenshot in der oben erwähnten Anleitung; Mitteilungen via Report CANCL/CANCT -> Status «<i>Processed</i>») sowie die technische Empfangsbestätigung gelten als Nachweis für eine erfolgreiche Übermittlung an die MROS. Die MROS behält sich vor, nicht korrekt oder unvollständig erfasste Abbruchmitteilungen zur Überarbeitung an den Finanzintermediär zurückzuweisen.

Haftung

Obwohl die Bundesbehörden mit aller Sorgfalt auf die Richtigkeit der veröffentlichten Informationen achtet, kann hinsichtlich der inhaltlichen Richtigkeit, Genauigkeit, Aktualität, Zuverlässigkeit und Vollständigkeit dieser Informationen keine Gewährleistung übernommen werden.

Die Bundesbehörden behalten sich ausdrücklich vor, jederzeit Inhalte ohne Ankündigung ganz oder teilweise zu ändern, zu löschen oder zeitweise nicht zu veröffentlichen.

Haftungsansprüche gegen die Bundesbehörden wegen Schäden materieller oder immaterieller Art, welche aus dem Zugriff oder der Nutzung bzw. Nichtnutzung der veröffentlichten Informationen, durch Missbrauch der Verbindung oder durch technische Störungen entstanden sind, werden ausgeschlossen.