



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2025



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2025

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Meldestelle für Geldwäscherei (MROS)
3003 Bern

Telefon: (+41) 58 463 40 40
E-Mail: meldestelle-geldwaescherei@fedpol.admin.ch

Internet: <http://www.fedpol.admin.ch>

Inhaltsverzeichnis

1	Vorwort	7
2	Wichtige strategische Entwicklungen	8
2.1	FATF-Länderprüfung – Vorschau	8
2.2	Die MROS im internationalen FIU-Vergleich	10
2.3	IT-Projekte und Tools	11
2.4	«Typologieberichte» und «Negativtypologien»	12
2.5	Public-Private-Partnership (PPP)	12
2.5.1	Swiss FIPPP	12
2.5.2	EFIPPP	13
2.6	Nationale Risikoanalyse (NRA)	14
2.7	Projekte und Veranstaltungen	15
2.7.1	Global FIU Leadership Conference	15
2.7.2	3 rd MROS Crypto-Symposium	15
2.7.3	Underground Banking Roundtable	16
2.7.4	Best Practice-Anlass	16
3	Jahresstatistik der Meldestelle	17
3.1	Gesamtübersicht 2025	17
3.2	Verdachtsmeldungen	18
3.3	Verdachtsmeldungen nach Branche der Meldepflichtigen	18
3.4	Rechtsgrundlage der Meldungen	20
3.5	Vortaten	20
3.6	Verdachtsauslösende Elemente	21
3.7	Anzeigen an die Strafverfolgungsbehörden	22
3.8	Rückmeldungen der Strafbehörden	24
3.9	Terrorismusfinanzierung	25
3.10	Organisierte Kriminalität	25
3.11	Verdachtsmeldungen mit Bezug zu virtuellen Währungen	26
3.12	Herausgabe von Informationen nach Artikel 11a GwG	27
3.13	Abbruchmeldungen nach Artikel 9b GwG	28
3.14	Informationsaustausch mit ausländischen FIUs	28
3.15	Informationsaustausch mit Schweizer Behörden	29
4	Trends	30
4.1	Betrug durch manipulierte Geschäftskommunikation	30
4.2	Schattenflotten	31
4.3	Italienische Mafia	33
5	Aus der Praxis der Meldestelle	35
5.1	Praxisänderung Abbruchmitteilungen – «De-minimis-Praxis»	35
5.1.1	Kernelemente der neuen Praxis	35
5.1.2	Rechtliche und praktische Grenzen der ex ante Abbruchmitteilung	35
5.2	Datenstandard	36
5.2.1	Datenstandard bei Verdachtsmeldungen	36
5.2.2	Gesetzliche Neuerung – Artikel 23 Absatz 7 GwG	36
5.2.3	Technische Umsetzung – Vorgehen und Perspektive	36
5.2.4	XML Data Quality Report	36

6	Internationale Zusammenarbeit in der Bekämpfung der Geldwäschei	38
6.1	Egmont-Gruppe	38
6.2	Financial Action Task Force (FATF)	38
6.3	Taskforces	39
6.4	Bilaterale Treffen	39
7	Organisation der MROS	40

1 Vorwort

Das Berichtsjahr 2025 war durch ein erneutes, deutliches Wachstum des Melde- und Datenvolumens geprägt. Im Jahr 2025 gingen bei der Meldestelle für Geldwäscherei (MROS) insgesamt 21 087 Verdachtsmeldungen ein, was einer Zunahme von 39,3% gegenüber dem Vorjahr entspricht. Damit erreichte das Meldeaufkommen einen neuen Höchststand. Durchschnittlich gingen 82 Verdachtsmeldungen pro Werktag ein. Seit der Einführung des Informationssystems goAML im Jahr 2020 hat sich das jährliche Meldevolumen nahezu vervierfacht. Der überwiegende Teil der Meldungen stammte auch 2025 aus dem Bankensektor (91,3%). Parallel zum Anstieg der eingehenden Meldungen nahm auch die operative Tätigkeit der MROS zu: 1375 Fälle wurden im Rahmen einer Anzeige an die zuständigen Strafverfolgungsbehörden übermittelt (+31,5% gegenüber 2024). Zudem intensivierte sich der Einsatz vertiefter Analyseinstrumente, namentlich durch Informationsanfragen nach Artikel 11a des Bundesgesetzes über die Bekämpfung der Geldwäscherei und Terrorismusfinanzierung (GwG; SR 955.0) sowie durch einen weiter zunehmenden nationalen und internationalen Informationsaustausch. Das stark wachsende Datenvolumen erhöhte die qualitativen Herausforderungen an MROS und damit die Anforderungen an Effizienz, Priorisierung und Datenqualität.

Vor diesem Hintergrund blieb die Tätigkeit der MROS konsequent risikobasiert und intelligencorientiert. Der Fokus lag unverändert auf Sachverhalten mit Bezug zu schwerer Kriminalität, insbesondere organisierter Kriminalität, Terrorismusfinanzierung, komplexen Betrugsdelikten, Korruption, Menschenhandel sowie Sanktionsumgehung. Die enge Zusammenarbeit mit den nationalen Strafverfolgungsbehörden, den Aufsichtsstellen und weiteren zuständigen Behörden, aber auch mit den internationalen Partnern bildet dabei eine zentrale Voraussetzung für die Wirksamkeit des schweizerischen Geldwäschereiabwehrdispositivs.

Von besonderer strategischer Bedeutung war im Berichtsjahr die Vorbereitung auf die fünfte Länderprüfung der Schweiz durch die Financial Action Task Force (FATF), die ab Ende 2026 durchgeführt wird. Der aktuelle Prüfzyklus der FATF legt einen verstärkten Schwerpunkt auf die Effektivität des Systems und dessen praktische Umsetzung. Der MROS

kommt dabei eine Schlüsselrolle zu. Aufgrund ihres gesetzlichen Auftrags und ihrer Scharnierfunktion zwischen Finanzmarkt und Strafverfolgung beeinflussen ihre Tätigkeiten die Bewertung zahlreicher Prüfkriterien.

Im internationalen Kontext intensivierte die MROS ihre Zusammenarbeit mit ausländischen Meldestellen sowie ihre Mitwirkung in multilateralen Gremien und Kooperationsformaten. Der grenzüberschreitende Informationsaustausch gewann weiter an Bedeutung, insbesondere vor dem Hintergrund zunehmend international organisierter Fallkomplexe und komplexer Finanzflüsse. Qualität, Geschwindigkeit und Verlässlichkeit dieses Austauschs sind entscheidend für die frühzeitige Sicherung von Vermögenswerten und die wirksame Unterstützung laufender Ermittlungen.

Ein weiterer Schwerpunkt lag in der Weiterentwicklung der technischen und organisatorischen Grundlagen der MROS. Abgeschlossene und laufende IT-Projekte zielten darauf ab, Prozesse zu standardisieren, die Effizienz der Fallbearbeitung zu erhöhen und die verfügbaren Daten besser für risikobasierte Analysen nutzbar zu machen. Gleichzeitig blieb die Sicherstellung einer hohen Daten- und Meldequalität eine zentrale Voraussetzung für die Wirksamkeit der Analysearbeit. Die entsprechenden Initiativen betreffen sowohl die internen Prozesse der MROS als auch die Schnittstelle zu den meldepflichtigen Akteuren.

Der Jahresbericht 2025 richtet sich an Behörden, Finanzintermediäre, politische Entscheidungsträgerinnen und Entscheidungsträger sowie an eine interessierte Fachöffentlichkeit. Er soll eine sachliche Grundlage für die Einordnung der dargestellten Entwicklungen bieten und zur weiteren Diskussion über die Ausgestaltung und Leistungsfähigkeit des schweizerischen Systems zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung beitragen.

2 Wichtige strategische Entwicklungen

2.1 FATF-Länderprüfung – Vorschau

Zwischen Ende 2026 und Januar 2028 wird die Schweiz von der FATF¹ zum fünften Mal im Rahmen einer sogenannten «Mutual Evaluation» geprüft.

Die FATF mit Sitz in Paris ist das zentrale internationale Gremium zur Festlegung von Standards zur Bekämpfung und Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung. In insgesamt 40 Empfehlungen² definiert sie einheitliche Anforderungen und Massstäbe, die sich an den gesamten Finanzsektor sowie an weitere relevante Personen und Berufsgruppen richten. Die Überprüfung der Umsetzung dieser Standards erfolgt im Rahmen periodischer Peer-Reviews, bei denen sich die FATF-Mitgliedstaaten gegenseitig evaluieren. Die Ergebnisse werden in einem Länderbericht (MER; Mutual Evaluation Report) festgehalten und mittels einer Einschätzung (Ratings) bewertet. Der Bericht wird von der FATF-Plenarversammlung verabschiedet, welche abhängig vom erreichten Rating Folgemassnahmen beschliessen kann.

Die FATF ist keine internationale Organisation im Sinne des Völkerrechts, sondern ein zwischenstaatliches politisches Gremium. Ihre Empfehlungen entfalten daher keine unmittelbare rechtliche Bindungswirkung für die Mitgliedstaaten. Gleichwohl besitzt sie faktisch erhebliche Bedeutung: Wer sich nicht an die Empfehlungen der FATF hält, wird von der FATF öffentlich an den Pranger gestellt. Die FATF veröffentlicht dreimal pro Jahr Listen³ zu Staaten mit strategischen Defiziten im Bereich der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung. Dabei wird zwischen Jurisdiktionen mit schwerwiegenden Mängeln, die ein erhöhtes Risiko für das internationale Finanzsystem darstellen, und solchen mit identifizierten Defiziten unterschieden: Auf der sogenannten «schwarzen Liste» führt die FATF jene Jurisdiktionen auf, die erhebliche strategische Defizite bei der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung aufweisen und die internationalen Bemühungen im Kampf dagegen erschweren oder gar verhindern. Auf der sogenannten

«grauen Liste» werden jene Jurisdiktionen aufgeführt, die strategische Defizite in ihren Systemen zur Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung aufweisen, sich jedoch verpflichtet haben, diese Mängel innerhalb vereinbarter Fristen in Zusammenarbeit mit der FATF zu beheben und deshalb einer verstärkten Überwachung unterliegen.

Die Aufnahme eines Landes in das Listing hat für andere Mitgliedstaaten regulatorische Konsequenzen, insbesondere die Pflicht zur Anwendung verstärkter risikomindernder Massnahmen. Banken und Investoren sind verpflichtet, den vom Listing betroffenen Finanzplatz als erhöhtes Risiko einzustufen. Dadurch wird eine Kettenreaktion ausgelöst, welche sich nachteilig auf die Reputation und die Attraktivität eines Finanzplatzes auswirkt. Für betroffene Finanzplätze resultieren daraus erhöhte Sorgfaltspflichten, verlängerte Abwicklungszeiten im Zahlungsverkehr, Einschränkungen oder der Abbau von Korrespondenzbankbeziehungen. Insbesondere Aktivitäten im Bereich der Handelsfinanzierungen sowie USD-Clearing-Beziehungen sind hiervon regelmässig betroffen. Empirische Untersuchungen zeigen, dass eine entsprechende Einstufung mit einem signifikanten Rückgang grenzüberschreitender Kapitalzuflüsse einhergehen kann. Exponierte Branchen müssen zudem regelmässig einen Wegzug beziehungsweise eine Verschiebung ihrer Aktivitäten ins Ausland ins Auge fassen, um konkurrenzfähig zu bleiben. Ein schlechtes Abschneiden bei der Länderprüfung kann somit schmerzhaft volkswirtschaftliche Konsequenzen nach sich ziehen.

Die Schweiz wurde letztmals vor 10 Jahren geprüft. Die FATF hat am 7. Dezember 2016 den vierten Länderbericht⁴ zur Schweiz veröffentlicht. In neun Bereichen stellte sie damals Defizite bei der Umsetzung einzelner Empfehlungen fest. Die Schweiz musste sich in der Folge einem sogenannten «enhanced follow-up» unterziehen, welcher im Herbst 2023 abgeschlossen wurde. Die FATF würdigte dabei die Fortschritte, welche die Schweiz insbesondere durch die im März 2021 verabschiedete Revision

¹ [Financial Action Taskforce \(FATF\)](#).

² [FATF-Empfehlungen](#).

³ [FATF-Listing](#).

⁴ [Mutual Evaluation Report of Switzerland, Dezember 2016](#).

des GwG gemacht hat. Bei sechs Empfehlungen, darunter diejenige betreffend Sorgfaltspflichten der Finanzintermediäre gegenüber Kunden, konnte die Schweiz die offenen Punkte weitgehend beheben.

Mit dem anstehenden fünften Prüfzyklus wird der Fokus der Länderprüfung stärker auf die Wirksamkeit des Systems (Effectiveness) zur Bekämpfung der Geldwäscherei, der Terrorismusfinanzierung und der Proliferationsfinanzierung gelegt. Neben der formellen Umsetzung der internationalen Standards in nationales Recht wird verstärkt geprüft, inwiefern diese in der Praxis effektiv angewendet werden. Als profunde Nachweise dienen insbesondere Statistiken (z. B. Anzahl Verdachtsmeldungen, Analysen, Strafverfahren, Verurteilungen, ergriffene Massnahmen, Informationen, die national und international ausgetauscht werden, etc.) und Case Studies, anhand derer die Zusammenarbeit zwischen Behörden und dem Privatsektor nachvollziehbar dargestellt und der «Erfolg» sichtbar gemacht wird.

Die Prüfung beginnt Ende 2026 und gliedert sich in zwei Teile. In einer ersten Phase nimmt ein aus sechs bis acht Expertinnen und Experten anderer Mitgliedsstaaten bestehendes Prüfteam eine Analyse der rechtlichen Grundlagen und der Umsetzung der 40 Empfehlungen ins nationale Recht vor. Diese Phase entspricht im Wesentlichen einem Dokumenten-Review. Der zweite Teil befasst sich mit der Effektivität des Abwehrdispositivs. Zentrale Bedeutung kommt dabei der sogenannten «On-site-visit» zu, einer dreiwöchigen Interviewphase im Frühsommer 2027, in deren Rahmen verschiedene Behörden, aber auch Vertreterinnen und Vertreter des Finanzmarktes, zur Funktionsweise und Wirksamkeit des Geldwäschereiabwehrdispositivs befragt werden. Nach Abschluss der Prüfung wird ein Berichtsentwurf erstellt, der in mehreren Stellungnahmen konsolidiert und schliesslich an der Plenarversammlung im Februar 2028 von den Mitgliedsländern verhandelt und verabschiedet wird. Die bisher im Rahmen des fünften Prüfzyklus publizierten Länderberichte⁵ deuten darauf hin, dass die FATF in der Bewertung der einzelnen Prüfpunkte eine strengere Praxis anwendet.

Die Effektivitätsprüfung umfasst insgesamt 11 Kapitel (sogenannte Immediate Outcomes – IO).

Jeder IO wird mit den Stufen High / Substantial / Moderate / Low Effectiveness bewertet, wobei die letzten beiden Stufen als ungenügend gelten.

Immediate Outcomes (IO) der FATF	
IO.1	Risiko, Politik & Koordination
IO.2	Internationale Zusammenarbeit
IO.3	Aufsicht über FI & VASPs
IO.4	Aufsicht über Designated Non-Financial Businesses and Professions (DNFBPs)
IO.5	Juristische Personen & Trusts
IO.6	Financial Intelligence
IO.7	Geldwäscherei Ermittlungen und Strafverfolgung
IO.8	Einziehung / Asset Recovery
IO.9	Terrorismusfinanzierung: Ermittlungen & Strafverfolgung
IO.10	Terrorismusfinanzierung: Präventive Massnahmen & Sanktionen
IO.11	Proliferationsfinanzierung

Der MROS kommt in der Länderprüfung eine zentrale Rolle zu. Mit IO.6 verfügt sie über ein eigenes Prüfkapitel. Aufgrund ihres gesetzlichen Auftrages (Financial Intelligence, Kooperation und Prävention) sowie ihrer Scharnierfunktion zwischen Finanzmarkt und Strafverfolgungsbehörden beeinflussen ihre Tätigkeiten jedoch zahlreiche weitere IO (un)mittelbar. Ein gutes Abschneiden der MROS ist daher von wesentlicher Bedeutung für das Gesamtergebnis der Länderprüfung. Im Rahmen der Länderprüfung durch die FATF sind auf nationaler Ebene sämtliche relevanten Behörden des Dispositivs zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung – namentlich Strafverfolgungsbehörden von Bund und Kantonen, Aufsichtsbehörden, Meldestelle für Geldwäscherei (MROS) sowie Zoll- und Steuerbehörden – in den Evaluationsprozess eingebunden, wobei das Staatssekretariat für internationale Finanzfragen (SIF) die Gesamtkoordination und Federführung für die Schweiz wahrnimmt. In Vorbereitung auf die Länderprüfung hat die MROS intern eine GAP-Analyse durchgeführt. Ziel war es, unter Berücksichtigung der Feststellungen aus der Länderprüfung 2016 sowie des aktuell geltenden FATF-Prüfkatalogs zu identifizieren, ob strukturelle oder operative Defizite bestehen. Die Resultate fliessen in die Vorbereitung der Prüfung ein.

⁵ Bisher durchgeführte Länderprüfungen im 5. Zyklus sind: Malaysia, Belgien, Singapur, Italien und Österreich.

2.2 Die MROS im internationalen FIU-Vergleich

Vor dem Hintergrund der anstehenden operativen und finanziellen Herausforderungen führte die MROS im Dezember 2024 und Januar 2025 eine Umfrage unter sechs hinsichtlich Grösse und Mandat vergleichbaren ausländischen Financial Intelligence Units (FIU) durch.⁶ Gegenstand der Befragung waren unter anderem aktuelle und zukünftige Herausforderungen, die Wirksamkeit von Massnahmen zur Sicherstellung der Datenqualität sowie die eingesetzten technischen Instrumente und die personelle Zusammensetzung. Im Zentrum der Erhebung stand die Frage, wo die FIUs die wesentlichen Herausforderungen verorten und mit welchen organisatorischen und technischen Ansätzen sie diesen begegnen. Gleichzeitig verfolgte die MROS das Ziel, den bestehenden internationalen Austausch zu vertiefen und einen gezielten Erfahrungsaustausch zu ausgewählten Fragestellungen zu etablieren.

Als zentrale Herausforderung identifizierte die überwiegende Mehrheit der befragten FIUs das anhaltende Wachstum des Melde- und Datenvolumens bei gleichzeitig begrenzten personellen und finanziellen Ressourcen. Ebenfalls von hoher Bedeutung sind die Entwicklungen und der effektive Einsatz geeigneter Analyseverfahren und -instrumente. Als wirksamste Massnahmen zur Bewältigung dieser Herausforderungen wurden insbesondere die Automatisierung von Arbeitsschritten, der Einsatz von Data-Science-Methoden sowie gezielte Prozessanpassungen genannt.

Mit dem steigenden Datenvolumen gewinnt zudem die Qualität der eingehenden Meldungen weiter an Bedeutung. Zur Verbesserung der Datenqualität haben die FIUs unterschiedliche Massnahmen implementiert. Dazu zählen einerseits systematische Ansätze des Datenqualitätsmonitorings sowie automatisierte und manuelle technische Verfahren zur Datenbereinigung. Andererseits setzen die FIUs auf regelmässige Schulungen der meldenden Finanzintermediäre sowie der internen Nutzerinnen und Nutzer der Datenbanksysteme. Zudem aktualisieren sie ihre Datenstandard- und Dokumentationsgrundlagen fortlaufend.

Hinsichtlich der eingesetzten technischen Lösungen verfolgen die befragten FIUs einen weitgehend vergleichbaren hybriden Ansatz. goAML ist dabei die zentrale Kernapplikation, ergänzt durch eigenentwickelte Anwendungen sowie durch Funktionen aus den Bereichen Data Engineering und Data Science, die mit Open-Source-Komponenten und kommerziellen Softwarelösungen kombiniert werden können.

Alle befragten FIUs gaben an, den gezielten Ausbau spezialisierter Stellenprofile mit Schwerpunkt Datenverarbeitung und Datenanalyse voranzutreiben. Genannt wurden insbesondere Funktionen wie Data Scientist, Software Engineer, Data Analyst, Knowledge Management Officer sowie Compliance Officer mit entsprechendem datenbezogenem Fokus.

Die Ergebnisse der Umfrage bestätigen die Erkenntnisse der MROS aus dem laufenden internationalen Austausch. Sie verdeutlichen, dass dem exponentiellen Wachstum der Verdachtsmeldungen nicht allein durch eine Ausweitung personeller Ressourcen begegnet werden kann. Erforderlich ist vielmehr eine integrierte Strategie, welche Prozessautomatisierung, Investitionen in eine zeitgemässe Data Engineering- und Data Science-Infrastruktur sowie den gezielten Aufbau zusätzlicher personeller Kompetenzen mit Schwerpunkt auf Datenprozessen und Datenanalysen kombiniert.

Im internationalen Vergleich mit anderen FIUs zeigt sich, dass die MROS – gemessen an der Grösse des Schweizer Finanzplatzes sowie den besonderen Risiken, die von der grenzüberschreitenden Vermögensverwaltung ausgehen – mit rund 57 Vollzeitstellen (FTE) über vergleichsweise begrenzte personelle Ressourcen verfügt. Andere relevante internationale und mit der Schweiz vergleichbare Finanzplätze (z. B. Luxemburg (80 FTE), Niederlande (110 FTE), Hong Kong (100 FTE)) weisen deutlich höhere personelle Kapazitäten in ihrer jeweiligen FIU auf.

⁶ FIU Belgien, FIU Finnland, FIU Niederlande, FIU Luxembourg, FIU Dänemark, FIU Hongkong.

2.3 IT-Projekte und Tools

Die Meldestelle verfolgt verschiedene IT-Projekte mit dem Ziel, ihre operativen Prozesse systematisch zu optimieren, zu standardisieren und ihre Analysefähigkeiten weiterzuentwickeln. Der Schwerpunkt liegt dabei auf der Effizienzsteigerung im Meldungseingang und in der Meldungsverarbeitung sowie auf der verbesserten Nutzung der verfügbaren Daten für risikobasierte Analysen. Im Jahr 2025 konnten mehrere Vorhaben abgeschlossen werden.

Zu den umgesetzten Neuerungen zählt die Einführung einer **automatisierten Empfangsbestätigung** für Verdachtsmeldungen. In Zusammenarbeit mit einem Softwarehersteller wurde eine Lösung entwickelt, welche die Empfangsbestätigung unmittelbar aus dem laufenden Bearbeitungsworkflow generiert. Dadurch entfällt das bisher notwendige manuelle Auslösen der Empfangsbestätigung. Die Anpassung trägt zur Reduktion des administrativen Aufwands in der Fallbearbeitung bei.

Eine weitere Effizienzsteigerung erreichte die MROS mit der Einführung eines neuen **Kurzübermittlungs-Templates**. Dieses ermöglicht eine vereinfachte und beschleunigte Übermittlung von Sachverhalten geringerer Komplexität an die Strafverfolgungsbehörden. Inhalte, die bislang ausserhalb von goAML unter Inkaufnahme mehrerer Medienbrüche erstellt werden mussten, können nun vollständig innerhalb von goAML und ohne Systemwechsel aufbereitet werden. Auch dies führt zu einer Reduktion des administrativen Aufwandes und zur Verkürzung zwischen dem Absetzen einer Verdachtsmeldung durch einen Finanzintermediären und der Übermittlung der relevanten Informationen an die kompetente Strafverfolgungsbehörde.

Im Zusammenhang mit der Bearbeitung der Amtshilfeanfragen führte die MROS ein **Abbrufverfahren** ein, das Strafverfolgungsbehörden und weiteren berechtigten Amtsstellen erlaubt, gezielte Abfragen in der goAML-Datenbank vorzunehmen. Im Rahmen sogenannter Hit-/No-Hit-Abfragen nach Artikel 35 Absatz 2 GwG erhalten die anfragenden Behörden Auskunft darüber, ob eine Person, ein Konto, eine Wallet-Adresse oder ein Unternehmen im Informationssystem goAML erfasst ist. Diese Vorabinformation dient der Einschätzung, ob eine formelle Amtshilfeanfrage zweckmässig ist. Ziel

des Verfahrens ist es, die Anzahl formeller Amtshilfeersuchen an die MROS als auch den administrativen Aufwand auf beiden Seiten zu reduzieren.

Neben den abgeschlossenen Vorhaben befinden sich weitere Projekte in der Umsetzungsphase. Diese sind auf zusätzliche Prozessoptimierungen sowie auf den Ausbau der Datenverarbeitungs- und Analysekapazitäten ausgerichtet. In diesem Zusammenhang arbeitet die MROS gemeinsam mit dem EJPD-ISC und fedpol an der **Weiterentwicklung ihrer technischen Infrastruktur**, um diese den Anforderungen eines zeitgemässen Data Engineerings und moderner Data-Science-Ansätze anzupassen. Diese erweiterte Infrastruktur bildet die Grundlage für die Umsetzung weiterer Projekte, darunter die weitgehend automatisierte Verarbeitung spezifischer Meldungstypen wie Money-Mule-Meldungen oder Meldungen im Zusammenhang mit Editionsverfügungen.

Ein weiteres zentrales Entwicklungsvorhaben betrifft den **Aufbau eines Report- und Risk-Scoring-Systems**. Ziel dieses Projekts ist es, gemeldete Objekte – insbesondere Personen, Konten, Unternehmen und Transaktionen – anhand definierter Kriterien risikobasiert zu klassifizieren. Dadurch soll die risikoorientierte Priorisierung von Meldungen weiter gestärkt und systematisiert werden. Eine erste Komponente dieses Gesamtsystems, das sogenannte Report Scoring, befindet sich derzeit in der Testphase. Das umfassendere Risk-Scoring-Modul wird aktuell entwickelt.

Die beschriebenen IT-Projekte und Weiterentwicklungen dienen insgesamt der Anpassung der technischen und organisatorischen Grundlagen der MROS an die Anforderungen eines zunehmend datengetriebenen Meldewesens. Durch die konsequente Automatisierung von Prozessen, den gezielten Ausbau moderner Analysefähigkeiten sowie die risikobasierte Ausrichtung der Meldungsbearbeitung wird die Effizienz erhöht, die Qualität der Analysen verbessert und die vorhandenen Ressourcen wirkungsvoller eingesetzt. Damit leistet die MROS einen substanziellen Beitrag zur Stärkung der Geldwäschereibekämpfung und zur wirksamen Unterstützung der Strafverfolgungsbehörden und weiterer zuständiger Stellen.

2.4 «Typologieberichte» und «Negativtypologien»

Die Sicherstellung einer hohen Daten- und Meldequalität bildete auch im Jahr 2025 einen zentralen Schwerpunkt der Tätigkeit der MROS. Während in den vergangenen Jahren vor allem formelle Mängel im Meldewesen im Vordergrund standen, ist zunehmend eine Abnahme der materiellen Qualität der Verdachtsmeldungen festzustellen. Vor diesem Hintergrund weist die MROS seit mehreren Jahren auf die zentrale Bedeutung einer hohen Daten- und Meldequalität hin, zuletzt im Jahresbericht 2024 (Kap. 5.1) sowie bereits in den Jahresberichten 2023 (Kap. 2.1 und 2.2) und 2022 (Kap. 2.3.5).

Zur Verbesserung der Meldequalität verfolgt die MROS einen mehrdimensionalen Ansatz: Neben dem direkten Austausch mit einzelnen Finanzintermediären setzt sie auf gezielte Sensibilisierungs- und Wissensvermittlungsformate, darunter Schulungen, Fachveranstaltungen und themenspezifische Publikationen. Eine zentrale Rolle spielen dabei die sogenannten «**Typologieberichte**», in denen anonymisierte Sachverhalte systematisch aufbereitet und anhand von Best-Practice-Beispielen konkrete Orientierungshilfen für die Durchführung von Abklärungen in typischen Konstellationen bereitgestellt werden. In diesem Kontext veröffentlichte die MROS im September 2025 den zweiten Typologiebericht mit dem thematischen Schwerpunkt «Enabler».

Ergänzend zu diesen Best-Practice-Typologien publizierte die MROS im August 2025 erstmals sogenannte «**Negativtypologien**». Dabei handelt es sich um stark vereinfachte Darstellungen ausgewählter Sachverhaltselemente, die wiederkehrende Schwachstellen bei den Verdachtsmeldungen veranschaulichen. Wie die Best-Practice-Typologien stellen auch die Negativtypologien weder eine Auslegungspraxis noch eine Handlungsanweisung dar. Sie dienen ausschliess-

lich der Sensibilisierung für typische Defizite und sollen Finanzintermediäre dazu anregen, sich vertieft mit dem Hintergrund von Geschäftsbeziehungen oder Transaktionen, der möglichen Vortat sowie dem geldwäschereirelevanten Gesamtsachverhalt auseinanderzusetzen. Eine fundierte, sorgfältig abgeklärte und nachvollziehbar dokumentierte Verdachtsmeldung bildet eine zentrale Voraussetzung für die wirksame Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung. Sie ist zugleich Voraussetzung für den sachgerechten Einsatz weiterentwickelter technologischer Instrumente, insbesondere datenbasierter Analyseverfahren sowie dem Einsatz moderner Analysesoftware. Die Verantwortung für die Beurteilung, ob ein konkreter Sachverhalt der Meldepflicht gemäss Artikel 9 GWG unterliegt, liegt in jedem Fall stets beim jeweiligen Finanzintermediär und ist im Einzelfall zu treffen.

2.5 Public-Private-Partnership (PPP)

2.5.1 Swiss FIPPP

Die Swiss Financial Intelligence Public Private Partnership («Swiss FIPPP») ist die strategische Partnerschaft zwischen der MROS und Schweizer Finanzinstituten aus dem Privatsektor. Ziel der Partnerschaft ist der strukturierte Informationsaustausch zur frühzeitigen Identifikation, Analyse und Einordnung von Risiken und Bedrohungen im Bereich der Geldwäscherei und der Terrorismusfinanzierung.

Die Swiss FIPPP nahm ihre Tätigkeit Ende 2024 auf. Der inhaltliche Fokus liegt auf der strategischen Analyse von Methoden, Trends und Entwicklungen relevanter Tatphänomene. Auf dieser Grundlage werden Erkennungsmerkmale (Indikatoren) sowie Beschreibungen neuer oder sich verändernder Modi Operandi (Typologien) erarbeitet, um potenzielle Bedrohungen rascher erkennen zu können. Der Informationsaustausch unterstützt den Privatsektor dabei, verdächtige Sachverhalte gezielter zu



Abbildung 1: Logo Swiss FIPPP.



Abbildung 2: Logo EFIPPP

identifizieren, während er den Behörden als Grundlage für präventive Massnahmen und für die Strafverfolgung dient.

Die Aktivitäten der Swiss FIPPP werden von einem Vorstand koordiniert, deren Mitglieder von der Plenarversammlung gewählt werden. Die organisatorische und kommunikative Unterstützung der Partnerschaft liegt bei der MROS. Im Jahr 2025 fanden insgesamt drei Plenarsitzungen statt, an denen sämtliche Mitglieder teilnahmen. Ergänzend dazu tagten regelmässig themenspezifische Arbeitsgruppen. Derzeit bestehen zwei Arbeitsgruppen: Die Arbeitsgruppe «Regulatory and Innovation» befasst sich mit technischen und prozessualen Fragestellungen, insbesondere mit der Datenqualität und der Verbesserung von Verdachtsmeldungen. Die Arbeitsgruppe «Threats and Typologies» setzt ihren thematischen Schwerpunkt im Jahr 2025 auf die Phänomene Menschenhandel und Betrug.

Über ihre Tätigkeiten und Erkenntnisse informiert die Swiss FIPPP gezielt und adressatengerecht. Im Dezember 2025 veröffentlichte sie einen Newsletter zum Thema Betrug im Zusammenhang mit virtuellen IBAN⁷. Mit der zunehmenden Verbreitung von virtuellen IBAN steigen die Möglichkeiten für Kriminelle, die Verwendung derselben betrügerisch zu missbrauchen. Der Newsletter soll das Bewusstsein für diese Art von Betrug schärfen und Finanzintermediären, die davon betroffen sein könnten, praktische Massnahmen aufzeigen, um den damit verbundenen Risiken zu begegnen.

Die Swiss FIPPP ist als dynamische und weiterentwicklungsfähige Partnerschaft ausgestaltet. Die Bedürfnisse der Mitglieder sowie die Entwicklungen im Finanzmarkt werden kontinuierlich analysiert. Dabei werden auch internationale Erfahrungen mit

vergleichbaren Public-Private-Partnership-Modellen berücksichtigt, die teilweise bereits Formen einer vertieften, auch operativen Zusammenarbeit vorsehen.

2.5.2 EFIPPP

Die MROS setzte im Jahr 2025 ihr Engagement im Europol Financial Intelligence Public Private Partnership (EFIPPP) fort. Die EFIPPP ist eine transnationale Kooperationsplattform, welche den strukturierten Austausch zwischen FIU, Strafverfolgungsbehörden, Aufsichtsstellen sowie ausgewählten Vertreterinnen und Vertretern des Privatsektors zum Ziel hat. Im Fokus stehen die Prävention und Bekämpfung komplexer Formen der Finanz- und Wirtschaftskriminalität.

Im Berichtsjahr nahm die MROS an mehreren Plenarversammlungen der EFIPPP teil. Diese befassten sich mit ausgewählten thematischen Schwerpunkten wie «*Underground Banking*» und «*Unmasking the financial footprints of synthetic drugs trafficking*». In die Diskussionen brachte die MROS insbesondere ihre Erfahrungen aus dem schweizerischen Meldesystem sowie Erkenntnisse aus der operativen und strategischen Analyse von Verdachtsmeldungen ein. Gleichzeitig ermöglichte die Teilnahme den Austausch zu bestehenden Ansätzen und Erfahrungen anderer Partner.

Auf strategischer Ebene war die MROS auch 2025 im Steering Committee der EFIPPP vertreten. In dieser Funktion wirkte sie an der inhaltlichen Ausrichtung der Plattform, der Festlegung thematischer Prioritäten sowie der Koordination der Arbeitsgruppen mit. Zudem beteiligte sie sich an der Weiterentwicklung der Zusammenarbeit zwischen öffentlichen Stellen und privaten Akteuren.

⁷ <https://www.fedpol.admin.ch/dam/en/sd-web/KBBXG1w-FxY/fippp-newsletter-2025-12.pdf>.

Die MROS arbeitet aktiv in den Arbeitsgruppen Trafficking in Human Beings (THB), Child Sexual Abuse and Exploitation (CSAE) und Professional Enablers mit. Zudem ist die MROS seit 2025 Co-Chair der Innovation Working Group.

Durch ihr fortgesetztes Engagement im EFIPP trägt die MROS zur internationalen Vernetzung sowie zum Erfahrungsaustausch bei und unterstützt die Weiterentwicklung gemeinsamer Ansätze zur Bekämpfung der Geldwäscherei, der Terrorismusfinanzierung und weiterer Erscheinungsformen schwerer Finanz- und Wirtschaftskriminalität.

2.6 Nationale Risikoanalyse (NRA)

Die Beurteilung der Risiken im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung bildet einen wesentlichen Bestandteil der gesamtschweizerischen Strategie zur Bekämpfung von Finanzkriminalität. Die Schweiz führt daher in regelmässigen Abständen nationale Risikoanalysen (National Risk Assessments, NRA) durch und veröffentlicht deren Ergebnisse. Neben zwei sektorübergreifenden NRA-Berichten aus dem Jahr 2015⁸ und 2021⁹ liegen zahlreiche sektorielle bzw. themenspezifische Risikoberichte vor.¹⁰

Auftraggeberin und verantwortlich für die Koordination der nationalen Risikoanalysen ist die Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei, der Terrorismusfinanzierung und der Proliferationsfinanzierung (KGGT). Die KGGT ist eine vom Bundesrat eingesetzte ständige Koordinationsplattform mit dem Auftrag, die schweizerische Politik in diesen Bereichen abzustimmen. Die MROS ist Mitglied der KGGT und nimmt als Leiterin der Untergruppe «Risikoanalyse» eine federführende Rolle bei der Erstellung der Risikoberichte ein.

Mitte 2026 wird die KGGT den sektoriellen Risikobericht «National Risk Assessment: Juristische Personen und Rechtsvereinbarungen», den die MROS in Zusammenarbeit mit Expertinnen und Experten

aus verschiedenen Verwaltungsbehörden erstellte, publizieren.

Juristische Personen, Trusts und ähnliche Strukturen spielen regelmässig eine zentrale Rolle in Geldwäscherei-Fällen. Die Risikoanalyse bestätigt weitgehend die Erkenntnisse einer 2017 veröffentlichten sektoriellen Risikoanalyse zu juristischen Personen. Nach wie vor sind mit ausländischen juristischen Personen und Rechtsvereinbarungen höhere Risiken verbunden als mit schweizerischen. Die Rechtsform ist dabei von untergeordneter Bedeutung. Massgeblich ist vielmehr, ob eine juristische Person einer effektiven operativen Tätigkeit nachgeht. Sitzgesellschaften weisen ein deutlich erhöhtes Missbrauchspotenzial auf, insbesondere wenn es sich um Mantelgesellschaften handelt. Komplexe, grenzüberschreitende Strukturen oder ein fehlender wirtschaftlicher Zweck erhöhen das Missbrauchspotenzial erheblich. In diesem Kontext kommen Anwältinnen, Notaren und Treuhändern, sofern sie in die Gründung oder Strukturierung entsprechender Konstruktionen eingebunden sind, eine besondere Bedeutung zu.

Gleichzeitig hat die Schweiz den regulatorischen Rahmen wesentlich gestärkt und gesetzliche Lücken geschlossen: Inhaberaktien wurden prinzipiell abgeschafft, Schweizer Handelsgesellschaften zur Führung eines Aktien- oder Anteilsverzeichnisses verpflichtet sowie Sanktionsmassnahmen in Zusammenhang mit dem Führen von Aktien- und Anteilsverzeichnissen und Verifizierungspflichten der Finanzintermediäre in Zusammenhang mit den Angaben zur wirtschaftlichen Berechtigung eingeführt. Diese Massnahmen sollen insbesondere die Risiken im Zusammenhang mit schweizerischen juristischen Personen, namentlich Aktiengesellschaften, reduzieren.

Mit der Verabschiedung des Bundesgesetzes über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen (TJPG) und der Revision des GwG im September 2025 hat die Schweiz ihr Abwehrdispositiv weiter ausgebaut. Diese Neuerungen zielen darauf

⁸ [Erste nationale Risikoanalyse \(NRA\) – Bericht über die nationale Beurteilung der Geldwäscherei und Terrorismusfinanzierungsrisiken in der Schweiz](#), Juni 2015.

⁹ [Zweite nationale Risikoanalyse \(NRA\) – Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz](#), Oktober 2021.

¹⁰ [Publikationen der Meldestelle für Geldwäscherei \(MROS\)](#).

ab, die Transparenz in- und ausländischer juristischer Personen zu erhöhen und den zuständigen Behörden einen effizienteren Zugang zu Informationen über wirtschaftlich berechnete Personen zu ermöglichen. Gleichzeitig werden auch gewisse Tätigkeiten von Beraterinnen und Anwälten neu vom GWG erfasst. Die Wirksamkeit der verabschiedeten Massnahmen im Rahmen des TJPG und der GWG-Revision ist in den Nachfolgejahren zu beobachten.

2.7 Projekte und Veranstaltungen

Im Jahr 2025 führte die MROS verschiedene nationale und internationale Fachveranstaltungen durch. Diese Formate ermöglichen einen vertrauensgeschützten Austausch zu aktuellen Entwicklungen und operativen Herausforderungen und stärken zugleich die grenzüberschreitende Kooperation. Sie leisten einen Beitrag zur frühzeitigen Identifikation neuer Risiken und Etablierung von effizienteren geldwäschereirelevanten Präventions- und Ermittlungsstrukturen – ein Mehrwert, der letztlich das gesamte Geldwäschereiabwehrsystem, einschliesslich des Finanzsektors, nachhaltig stärkt.

2.7.1 Global FIU Leadership Conference

Vom 14. bis 15. Oktober 2025 war die MROS Gastgeberin der Global FIU Leadership Conference. Die Durchführung erfolgte in Zusammenarbeit mit ECOFEL¹¹ als Mitveranstalterin sowie mit Unterstützung des Staatssekretariats für Wirtschaft (SECO). Die Konferenz diente dem Austausch unter Führungskräften von Financial Intelligence Units (FIUs) und ergänzte die bestehenden Austauschformate der internationalen FIU-Zusammenarbeit.

Vor dem Hintergrund einer sich verändernden Finanz- und Technologielandschaft befassen sich FIUs zunehmend mit komplexen Analyse- und Koordinationsaufgaben. Internationale Entwicklungen, technologische Innovationen sowie steigende Meldevolumen stellen vergleichbare Anforderungen an zahlreiche FIUs.

Die Konferenz behandelte strategische Fragestellungen der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung. Thematisiert wurden unter anderem Entwicklungen im Bereich der

Informationstechnologie und der künstlichen Intelligenz, organisatorische Fragestellungen sowie mittel- und langfristige Perspektiven für FIUs. Der Austausch betraf insbesondere Fragen der Ausgestaltung interner Prozesse, der Nutzung technischer Instrumente sowie der internationalen Zusammenarbeit.

Die Veranstaltung stand unter dem Leitmotiv «Back to the Future» und bot einen Rahmen für die Diskussion bestehender Strukturen sowie möglicher Weiterentwicklungen der internationalen Financial-Intelligence-Architektur.

2.7.2 3rd MROS Crypto-Symposium

Am 3. November 2025 führte die MROS das dritte Crypto-Symposium durch. Rund 280 Vertreterinnen und Vertreter aus Behörden, dem Finanzsektor sowie aus internationalen Organisationen nahmen teil. Die Veranstaltung befasste sich mit Fragen der Effizienz im Umgang mit kryptobezogenen Risiken im Bereich der Geldwäscherei und Terrorismusfinanzierung.

Zu Beginn vermittelten Fachreferierende des World Economic Forum (Cybercrime Atlas) sowie von Europol einen Überblick über internationale Kooperationsansätze bei der Bekämpfung von Cyber- und Finanzkriminalität. Der Schwerpunkt lag auf grenzüberschreitenden Kooperationsmechanismen. Ein Vertreter der Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen erläuterte technische Abhängigkeiten bei der Bekämpfung von Finanzkriminalität. Thematisiert wurden insbesondere die Nutzung spezialisierter Analysetools sowie Fragen der Transparenz und Kontrolle technischer Systeme. Die MROS stellte nationale Typologien und aktuelle Entwicklungen im Kryptobereich vor. Der Nachmittag war Fallbeispielen gewidmet. Die FIU Kasachstan präsentierte eine Fallstudie zu einem grenzüberschreitenden Ponzi-System. Das US-amerikanische Technologieunternehmen TRM Labs behandelte kryptobezogene Sachverhalte im Zusammenhang mit sexualisierter Gewalt an Kindern. Die FIU der Vereinigten Arabischen Emirate sowie das Bundeskriminalamt Österreich stellten weitere praxisbezogene Analysen vor.

¹¹ ECOFEL als Teil der Egmont Group, unterstützt die Egmont-Mitglieder unter anderem gezielt mit Massnahmen zum Kapazitätsaufbau wie der Entwicklung von Führungskräften, E-Learnings, speziellen Schulungen.

Ein Panel mit Vertreterinnen und Vertretern aus dem öffentlichen und privaten Sektor schloss die Veranstaltung ab. Diskutiert wurden Kooperationsfragen, der Informationsaustausch sowie operative Herausforderungen.

Am Folgetag fand zudem ein behördeninterner Austausch zu operativen und technischen Fragestellungen statt.

2.7.3 Underground Banking Roundtable

Vom 20. bis 21. November 2025 fand in Bern der zweite Underground Banking Roundtable statt. Der Begriff Underground Banking bezeichnet informelle Finanzsysteme ausserhalb des regulierten Bankensektors, die grenzüberschreitende Transfers ohne Einbindung regulierter Institute ermöglichen.¹²

Solche Systeme bestehen in unterschiedlichen Ausprägungen seit langer Zeit und können sowohl legale als auch illegale Zwecke verfolgen. Aktuelle Analysen und Ermittlungen befassen sich insbesondere mit digitalisierten Erscheinungsformen.

Rund 80 Vertreterinnen und Vertreter von Strafverfolgungsbehörden und FIUs nahmen teil. Beiträge von INTERPOL, Europol, der Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) sowie dem United Nations Office on Drugs and Crime (UNODC) behandelten Typologien, operative Entwicklungen und Fallbeispiele. Die Teilnehmenden erörterten zudem praktische Herausforderungen und mögliche Ermittlungsansätze.

2.7.4 Best Practice-Anlass

Im Herbst 2025 führte die MROS gemeinsam mit der Schweizerischen Bankiervereinigung (SBVg) ein Fachseminar zum Thema «Best Practice beim Erstellen von Verdachtsmeldungen aus Sicht MROS» durch.

Die Veranstaltung vermittelte einen Überblick über Auftrag, Funktion und Arbeitsweise der MROS sowie über die Entwicklung des geldwäschereirechtlichen Dispositivs. Ein Schwerpunkt lag auf der analytischen Arbeitsweise der MROS und den dafür relevanten Informationsgrundlagen. Thematisiert wurde insbesondere die Bedeutung voll-

ständiger und strukturierter Angaben in Verdachtsmeldungen. Zudem behandelte das Seminar die Abklärungen nach Artikel 6 GwG, da die MROS selbst keine direkten Abklärungen gegenüber gemeldeten Personen vornimmt. Weiter wurden Fragen des institutionellen Austauschs sowie datenschutzrechtliche Rahmenbedingungen erörtert. Der Anlass diente dem fachlichen Austausch zwischen Finanzintermediären und Behörden im Rahmen der bestehenden gesetzlichen Vorgaben.

¹² [Underground Banking](#).

3 Jahresstatistik der Meldestelle

Die Meldestelle erstellt anonymisierte Statistiken zur Auswertung von Informationen über Geldwäscherei, deren Vortaten, organisierte Kriminalität sowie Terrorismusfinanzierung im jeweiligen Geschäftsjahr.¹³ Die statistischen Auswertungen umfassen insbesondere die bei der MROS eingegangenen Verdachtsmeldungen der Finanzintermediäre, Auskunftsbegehren zuständiger ausländischer Behörden sowie die Verfahren, die sich aus den Meldungen ergeben (vgl. Art. 23 MGwV¹⁴).

3.1 Gesamtübersicht 2025

- Im Berichtsjahr 2025 gingen bei der MROS insgesamt **21 087** Verdachtsmeldungen ein, was einem Durchschnitt von 82 Meldungen pro Werktag entspricht. Gegenüber dem Vorjahr nahm die Anzahl der eingereichten Verdachtsmeldungen um **39,3%** zu (2024: 15 141). Seit der Einführung des Informationssystems goAML im Januar 2020 hat sich das Meldevolumen damit nahezu vervierfacht. **91,3%** der im Jahr 2025 übermittelten Verdachtsmeldungen stammten von Finanzintermediären aus dem **Bankensektor** (Ø 2016 – 2025: 90,1%).
- Die MROS übermittelte im Jahr 2025 insgesamt **1375** Fälle an die **Strafverfolgungsbehörden**. Dies entspricht einer Zunahme von **31,5%** gegenüber dem Vorjahr. Den Strafverfolgungsbehörden wird jeweils ein Analysebericht mit den relevanten Informationen übermittelt. Eine Übermittlung kann auf mehreren Verdachtsmeldungen und Informationen beruhen, die nicht zwingend im selben Kalenderjahr bei der MROS eingegangen sind. Die Informationen können von unterschiedlichen in- und ausländischen Behörden stammen.
- Im Rahmen ihrer vertieften Analysearbeit stellte die MROS 2025 **1096 Anfragen** an meldende Finanzintermediäre oder Drittintermediäre **zur Herausgabe von Informationen nach Artikel 11a GwG**. Dies entspricht einer **Zunahme von 7,9%** gegenüber dem Vorjahr. In 20,1% der an die Strafverfolgungsbehörden übermittelten Fälle flossen zusätzliche Informationen ein, die von der MROS bei Finanzintermediären eingeholt worden waren.
- Der nationale Informationsaustausch zwischen der MROS und anderen Schweizer Behörden nahm im Jahr 2025 weiter zu. Die Anzahl der **spontanen Informationsübermittlungen** der MROS an andere inländische Behörden stieg gegenüber dem Vorjahr **um 36,9% auf 490**. Gleichzeitig übermittelten Schweizer Behörden der MROS vermehrt spontan Informationen (2025: **120; +13,2%** gegenüber Vorjahr) und richteten häufiger Auskunftsbegehren an die MROS (2025: **498; +11,4%** gegenüber Vorjahr).
- Im **internationalen Austausch** mit ausländischen FIUs zeigte sich im Jahr 2025 eine unterschiedliche Entwicklung. Die Anzahl der bei der MROS eingegangenen Auskunftsersuchen ausländischer FIUs ging gegenüber dem Vorjahr **um 15,1% auf 660 zurück**, während die Anzahl der **eingegangenen Spontaninformationen um 24,1% auf 932 zunahm**. Die MROS richtete ihrerseits 236 Auskunftsersuchen an ausländische FIUs (–1,3% gegenüber Vorjahr) und übermittelte 223 Spontaninformationen (+6,6% gegenüber Vorjahr).

¹³ Geschäftsjahr: 1. Januar bis 31. Dezember des jeweiligen Jahres.

¹⁴ Verordnung über die Meldestelle für Geldwäscherei (MGwV), SR 955.23.

3.2 Verdachtsmeldungen

Im Jahr 2025 gingen bei der MROS durchschnittlich 82 Verdachtsmeldungen pro Werktag ein. Insgesamt erhielt die MROS im Berichtsjahr 21 087 Verdachtsmeldungen von Finanzintermediären sowie Händlerinnen und Händlern. Dies entspricht einer Zunahme von 39,3% gegenüber dem Vorjahr. Seit der Einführung des Informationssystems goAML im Jahr 2020 hat sich die Anzahl der übermittelten Verdachtsmeldungen damit nahezu vervielfacht (vgl. Abbildung 3).¹⁵

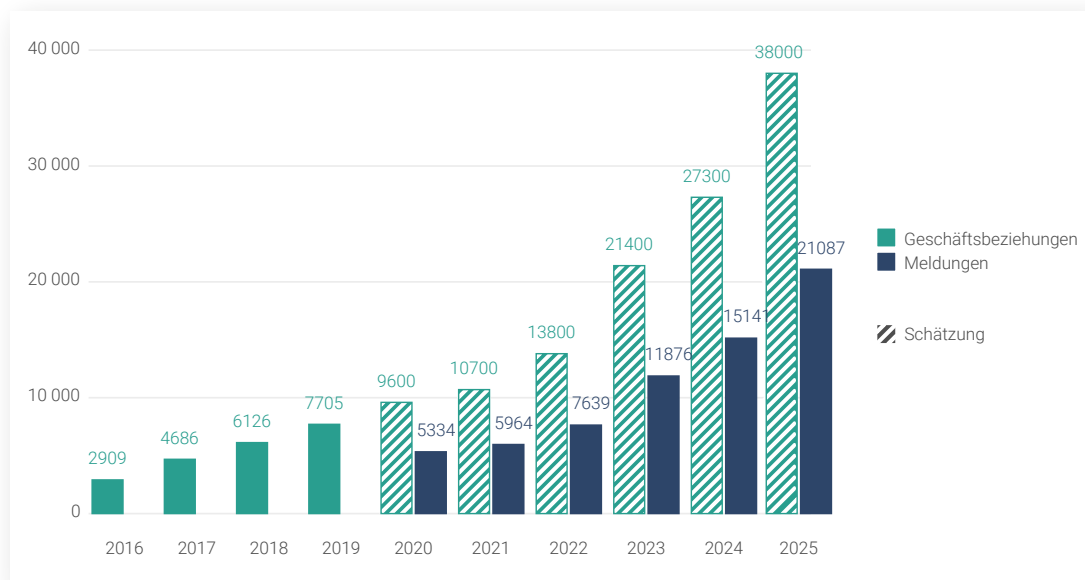
Wie Abbildung 3 zeigt, ist die Anzahl der jährlich gemeldeten Geschäftsbeziehungen aktuell 13mal höher als 2016: Während der MROS im Jahr 2016 insgesamt 2909 verdächtige Geschäftsbeziehungen gemeldet wurden, belief sich diese Zahl im Jahr 2025 auf hochgerechnet rund 38 000. Diese Entwicklung ist unter anderem auf ein erhöhtes Meldeaufkommen zurückzuführen, das

im Zusammenhang mit rechtlichen Anpassungen sowie mit Fortschritten in der Digitalisierung steht, insbesondere im Bereich des Transaktionsmonitorings und der internen Analyseprozesse bei den Finanzintermediären (z. B. durch verbesserte Tools).¹⁶

3.3 Verdachtsmeldungen nach Branche der Meldepflichtigen

Im Jahr 2025 entfielen 91,3% der bei der MROS eingegangenen Verdachtsmeldungen auf Finanzintermediäre aus dem Bankensektor. Das Meldeverhalten dieser Finanzintermediäre beeinflusst massgeblich die Anzahl und Art der Meldungen, die bei der MROS eingehen. Seit der Einführung des Informationssystems goAML hat sich die branchenbezogene Verteilung der Verdachtsmeldungen weitgehend stabil gezeigt (vgl. Tabelle 1).¹⁷

Abbildung 3: Anzahl gemeldete Geschäftsbeziehungen und Verdachtsmeldungen 2016 – 2025



¹⁵ Mit der Einführung von goAML wurde die Zählweise der Verdachtsfälle angepasst. Um dennoch einen Vergleich mit den Vorjahren zu ermöglichen, wird in Abbildung 3 die durchschnittliche Anzahl gemeldeter Geschäftsbeziehungen pro Verdachtsmeldung im Geschäftsjahr 2019 angewendet. Diese beläuft sich auf 1,8. Das bedeutet, dass die 21 087 Verdachtsmeldungen im Jahr 2025 geschätzt rund 38 000 Geschäftsbeziehungen entsprechen.

¹⁶ Vgl. Ausführungen im [Jahresbericht MROS 2023](#), Kap. 2.1.

¹⁷ Die Klassifizierung nach Branche erfolgt im goAML-Registrierungsprozess durch den Finanzintermediär selbst. Anschliessend überprüft die MROS im Rahmen eines Plausibilitätschecks, ob die Einstufung korrekt ist. Dies geschieht anhand der öffentlichen FINMA-Listen oder mittels Angaben einer SRO-Webseite, die Rückschlüsse auf die Branche erlaubt. Eine zu grobe Klassifizierung bleibt jedoch möglich, insbesondere in heterogenen Branchen wie der Vermögensverwaltung.

Tabelle 1: Verdachtsmeldungen nach Branche 2016 – 2025¹⁸

Branche	2016	2017 ^A	2018 ^A	2019 ^A	2020 ^B	2021 ^B	2022 ^B	2023 ^B	2024 ^B	2025 ^B	2025 in absoluten Zahlen	Durchschnitt 2016 – 2025
Banken	86%	91%	88,8%	89,9%	89,5%	90%	91,6%	90,5%	92,3%	91,3%	19 246	90,1%
Zahlungsverkehrsdienstleister	4,4%	3,1%	4,4%	4%	3,5%	2,5%	2%	2,8%	2,2%	2,6%	545	3,2%
Übrige Finanzintermediäre	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2%	0,2%	2,1%	446	1,5%
VASP / FinTech									1,5%	1,3%	276	1,4%
Kreditkartenanbieter	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	1,6%	1,3%	275	1,3%
Casinos	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	0,3%	0,3%	68	0,5%
Vermögensverwaltung	2,2%	1,9%	1%	0,9%	0,8%	1%	0,6%	0,8%	0,9%	0,3%	65	1%
Kredit-, Leasing-, Factoring- + Forfaitierungsgeschäfte	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	0,2%	0,2%	41	0,3%
Treuhänder	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	0,2%	0,2%	36	0,6%
Wertpapierhäuser	0,1%	0,3%	0,1%	0,3%	0%	0,2%	0,1%	0,2%	0,2%	0,1%	30	0,2%
Versicherungen	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	0,2%	0,1%	26	0,6%
Rohwaren- und Edelmetallhandel	0,1%	0,2%	0%	0,3%	0,2%	0,5%	0,3%	0,3%	0,2%	0,1%	20	0,2%
Geldwechsel/Change	0%	0%	0%	0%	0,1%	0,1%	0,3%	0,6%	0%	0%	4	0,1%
SRO	0%	0%	0%	0,1%	0%	0%	0%	0,1%	0%	0%	3	0%
Devisenhandel	0,1%	0%	0%	0,3%	0%	0%	0%	0%	0%	0%	2	0%
Rechtsanwälte und Notare	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0%	0,1%	0%	0%	2	0,1%
Vertriebsträger von Anlagefonds	0%	0,1%	0%	0%	0%	0%	0%	0%	0%	0%	1	0%
Behörden (FINMA/ESBK/GESPA und interkantonale Behörden)	0%	0%	0%	0%	0%	0,1%	0%	0%	0%	0%	1	0%
Trustees	0%	0%	0%	0%	0,1%	0,1%	0%	0%	0%	0%	0	0%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	21 087	100,0%

^A Nach alter Zählweise (Geschäftsbeziehung)

^B Nach neuer Zählweise (Meldungen)

Seit dem Jahr 2024 werden Virtual Asset Service Provider (VASP) und FinTech-Anbieter statistisch als eigene Kategorie ausgewiesen. Im Berichtsjahr 2025 reichten VASP und FinTech-Finanzintermediäre 276 Verdachtsmeldungen bei der MROS ein (1,3%), was ein Minus von 0,2% gegenüber dem Vorjahr darstellt.

¹⁸ Die absoluten Zahlen für die Jahre 2016 – 2024 sind in den Jahresberichten der MROS der entsprechenden Jahre veröffentlicht.

3.4 Rechtsgrundlage der Meldungen

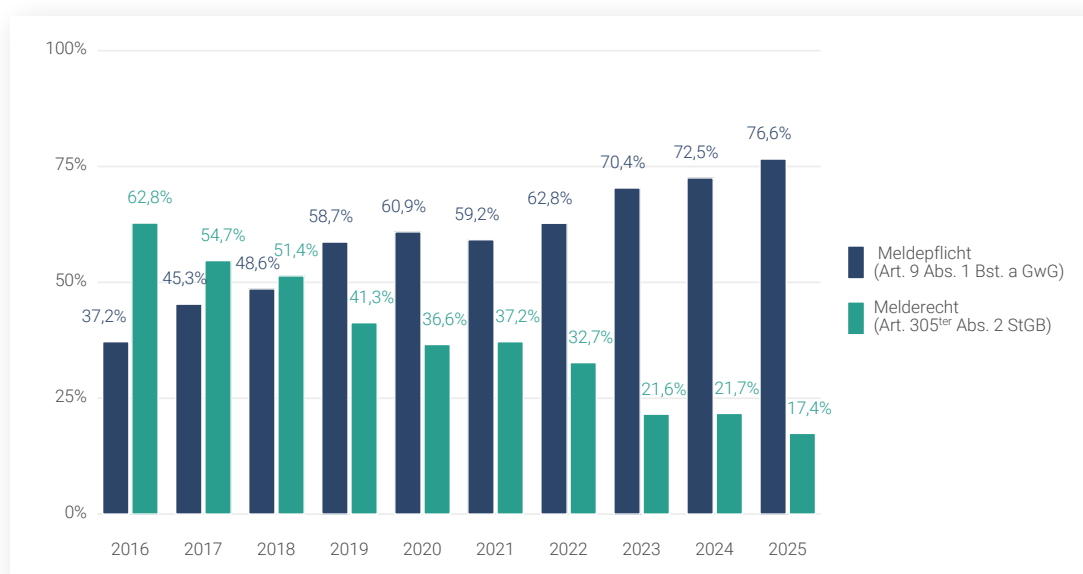
Die Rechtsgrundlage für eine Verdachtsmeldung ist abhängig vom Verdachtsgrad. Liegt ein begründeter Verdacht vor, sind Finanzintermediäre nach Artikel 9 Absatz 1 Buchstabe a GwG¹⁹ verpflichtet, der MROS eine Verdachtsmeldung zu erstatten. Bei einem einfachem Verdacht können die Finanzintermediäre vom Melderecht nach Artikel 305^{ter} Absatz 2 StGB²⁰ Gebrauch machen. Im Berichtsjahr 2025 erfolgten 76,6% der eingereichten Verdachtsmeldungen auf Grundlage der Meldepflicht (Art. 9 Abs. 1 Bst. a GwG, vgl. Abbildung 4). In 17,4% der Fälle stützten sich die Finanzintermediäre auf das Melderecht nach Artikel 305^{ter} Absatz 2 StGB. In weiteren 5,7% der Meldungen gaben die Finanzintermediäre an, dass sie Verhandlungen zur Aufnahme einer Geschäftsbeziehung wegen eines begründeten Verdachts nach Artikel 9 Absatz 1 Buchstabe a GwG abgebrochen hätten (Art. 9 Abs. 1 Bst. b GwG; nicht in Abbildung).²¹

Seit dem Jahr 2018 ist eine zunehmende Anwendung der Meldepflicht gegenüber dem Melderecht festzustellen, mit einem besonders ausgeprägten Anstieg im Jahr 2023 (vgl. Jahresbericht MROS 2023, Kap. 4.4). Auch im Berichtsjahr 2025 zeigte sich eine weitere Verschiebung zugunsten der Meldepflicht bei bestehenden Geschäftsbeziehungen (+4,1%), während das Melderecht entsprechend seltener angewendet wurde (-4,3%). Unverändert blieb demgegenüber der Anteil der Meldungen, die im Zusammenhang mit dem Abbruch von Verhandlungen zur Aufnahme einer neuen Geschäftsbeziehung gemäss Artikel 9 Absatz 1 Buchstabe b GwG erstattet wurden (+0,1%).

3.5 Vortaten

Finanzintermediäre geben im Rahmen einer Verdachtsmeldung jeweils an, welche Vortat(en) sie vermuten. Im Berichtsjahr 2025 wurde Betrug am

Abbildung 4: Meldungen bei bestehender Geschäftsbeziehung nach Rechtsgrundlage
2016 – 2025



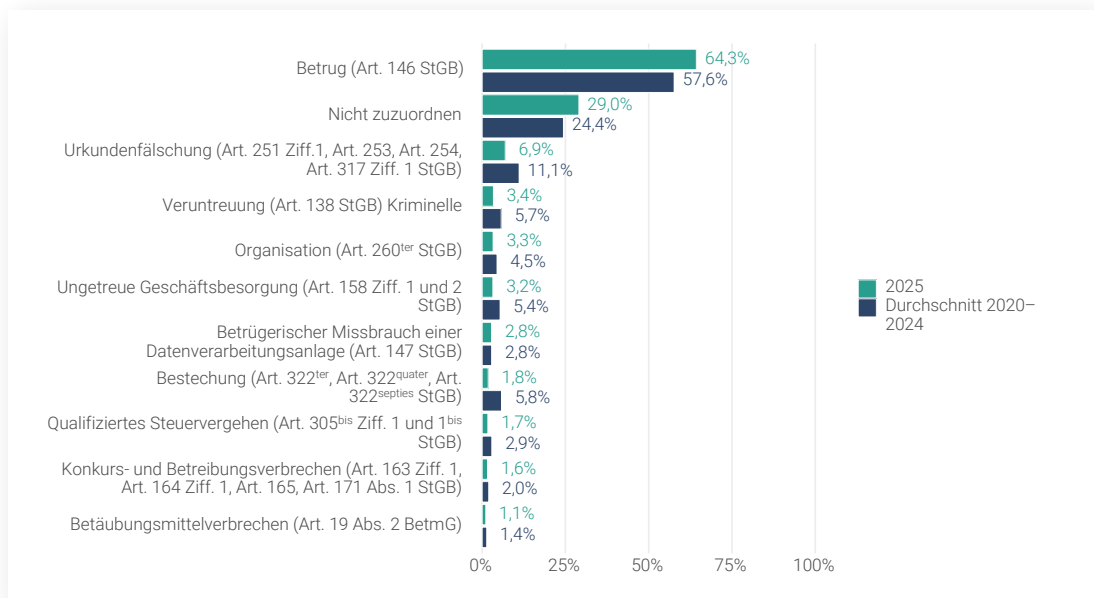
¹⁹ Art. 9 Abs. 1 Bst. a GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Art. 23 (Meldestelle) unverzüglich Meldung erstatten, wenn er weiss oder den begründeten Verdacht hat, dass die in die Geschäftsbeziehung involvierten Vermögenswerte (1.) im Zusammenhang mit einer strafbaren Handlung nach Art. 260^{ter} oder 305^{bis} StGB stehen, (2.) aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Art. 305^{bis} Ziffer 1^{bis} StGB herrühren, (3.) der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen, oder (4.) der Terrorismusfinanzierung (Art. 260^{quingies} Abs. 1 StGB) dienen.

²⁰ Schweizerisches Strafgesetzbuch, SR 311.0; Art. 305^{ter} Abs. 2 StGB: Die von Abs. 1 erfassten Personen sind berechtigt, der Meldestelle für Geldwäscherei im Bundesamt für Polizei Wahrnehmungen zu melden, die darauf schliessen lassen, dass Vermögenswerte aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Art. 305^{bis} Ziff. 1^{bis} herrühren.

²¹ Art. 9 Abs. 1 Bst. b GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Art. 23 (Meldestelle) unverzüglich Meldung erstatten, wenn er Verhandlungen zur Aufnahme einer Geschäftsbeziehung wegen eines begründeten Verdachts nach Art. 9 Abs. 1 Bst. a GwG abbricht.

Abbildung 5: Häufigkeit der vermuteten Vortaten

2020 – 2025, Häufigkeitsauswahl, Nennungen in % an Total aller Meldungen (Mehrfachnennungen möglich)



häufigsten als mutmassliche Vortat genannt. In 64,3% der Verdachtsmeldungen wurde Betrug entweder als alleinige Vortat oder in Kombination mit weiteren Delikten angegeben. Damit lag der Anteil über dem Durchschnitt der Jahre seit Einführung des Informationssystems goAML (Ø 2020 – 2024: 57,6%, vgl. Abbildung 5).²² Andere Vortaten wurden demgegenüber deutlich seltener angegeben. Am häufigsten nannten die Finanzintermediäre Urkundenfälschung (6,9%; Ø 2020 – 2024: 11,1%) und/oder Veruntreuung (3,4%; Ø 2020 – 2024: 5,7%). Der Anteil dieser Vortaten an den Verdachtsmeldungen nahm im Vergleich zu den Vorjahren weiter ab.

Die Angaben der Finanzintermediäre zu den vermuteten Vortaten stellen eine erste wichtige Qualifikation aufgrund der von den Finanzintermediären getätigten Abklärungen dar. Die vorstehende Abbildung zeigt, welche Straftaten die Finanzintermediäre zum Zeitpunkt der Einreichung der Ver-

dachtsmeldung vermuten. Im Rahmen der Analyse durch die MROS kann sich ergeben, dass der Verdacht auf eine andere Straftat fällt.²³

Im Berichtsjahr 2025 gaben die Meldepflichtigen bei 29,0% der Verdachtsmeldungen an, keine Vortat zuordnen zu können. Dieser Anteil hat sich über die vergangenen Jahre schrittweise erhöht und für die MROS weitreichende Folgen. Verdachtsmeldungen ohne Zuordnung einer Vortat erfordern seitens der MROS vertiefte Abklärungen, um die mutmassliche Vortat bestimmen zu können.

3.6 Verdachtsauslösende Elemente

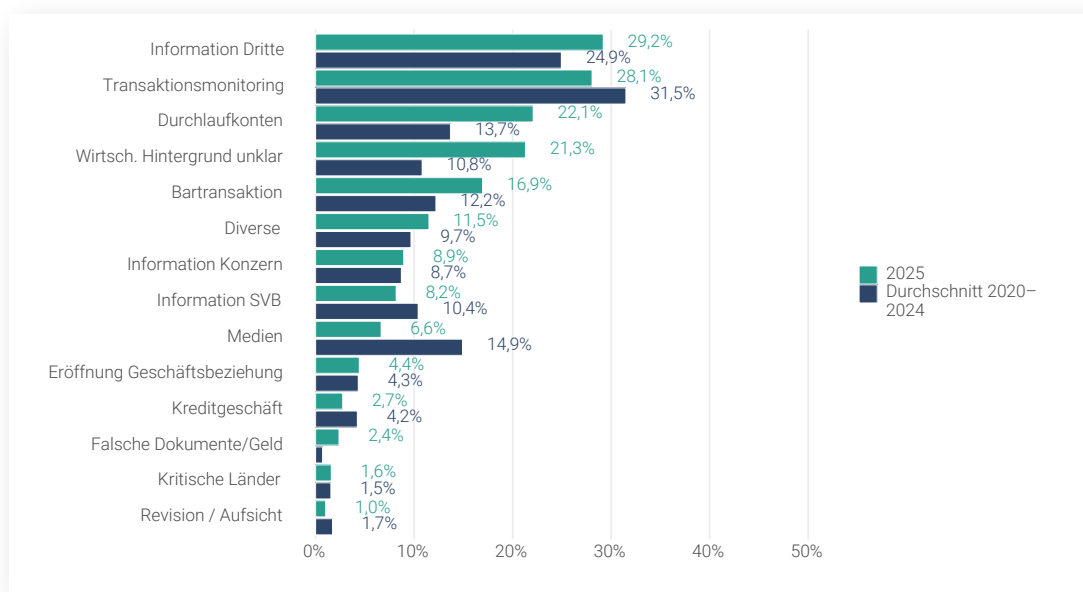
Verdachtsmeldungen an die MROS werden in der Regel aufgrund externer Informationsquellen oder interner Überwachungsprozesse erstattet. Im Berichtsjahr 2025 stützten sich die Finanzintermediäre bei 29,2% der Meldungen auf Informationen Dritter (Ø 2020 – 2024: 24,9%) und bei 28,1% auf

²² Mit der Einführung von goAML 2020 sind Mehrfachnennungen möglich. Ein Vergleich mit den Statistiken vor 2020 ist deshalb nicht möglich.

²³ Eine detailliertere Analyse zu den verschiedenen Geldwäschereivortaten wurde 2021 unter der Federführung der KGGT vorgenommen. [Zweite nationale Risikoanalyse \(NRA\) – Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz](#), Oktober 2021, S. 25 – 29.

Abbildung 6: Wichtige Verdachtsauslöser

2020 – 2025, Häufigkeitsauswahl, Nennungen in % an Total aller Meldungen (Mehrfachnennungen möglich)



Erkenntnisse aus dem Transaktionsmonitoring (\emptyset 2020 – 2024: 31,5%; vgl. Abbildung 6).²⁴ Daneben gewannen im Jahr 2025 weitere auslösende Elemente an Bedeutung. So wurden Durchlaufkonten in 22,1% der Verdachtsmeldungen als Auslöser angegeben, während ein unklarer wirtschaftlicher Hintergrund in 21,3% der Fälle genannt wurde (\emptyset 2020 – 2024: 13,7% bzw. 10,8%). Zudem wurden Bargeldtransaktionen im Berichtsjahr häufiger als verdachtsauslösendes Element gemeldet (2025: 16,9%, \emptyset 2020 – 2024: 12,2%).

3.7 Anzeigen an die Strafverfolgungsbehörden

Im Berichtsjahr 2025 übermittelte die MROS gestützt auf Artikel 23 Absatz 4 GwG 1375 Anzeigen an die Strafverfolgungsbehörden. Gegenüber dem Vorjahr entspricht dies einer Zunahme von 31,5% (2024: 1046). In den vergangenen Jahren haben sich die von der MROS übermittelten Anzeigen an die Strafverfolgungsbehörden inhaltlich zunehmend erweitert: Während im Jahr 2022 einer Anzeige durchschnittlich 1,4 Verdachtsmeldungen zugrunde lagen, enthielten die im Jahr 2025

übermittelten Anzeigen im Mittel 2,2 Verdachtsmeldungen. Dabei wurden vier ausserordentliche Fälle, in denen jeweils mehr als 500 Verdachtsmeldungen in eine Anzeige eingeflossen waren, nicht berücksichtigt.

Die 1375 übermittelten Anzeigen enthielten Informationen aus:

- 4414 im Jahr 2025 eingegangenen Meldungen, davon 3500, die in vier Anzeigen zusammengefasst wurden
- 1907 im Jahr 2024 eingegangenen Verdachtsmeldungen
- 79 im Jahr 2023 eingegangenen Verdachtsmeldungen
- 20 im Jahr 2022 eingegangenen Verdachtsmeldungen
- 13 im Jahr 2021 eingegangenen Verdachtsmeldungen und
- 28 vor dem Jahr 2021 eingegangenen Verdachtsmeldungen bzw. gemeldete Geschäftsbeziehungen

Die MROS übermittelte 90,5% der Anzeigen an die kantonalen Staatsanwaltschaften, 9,5% gingen an

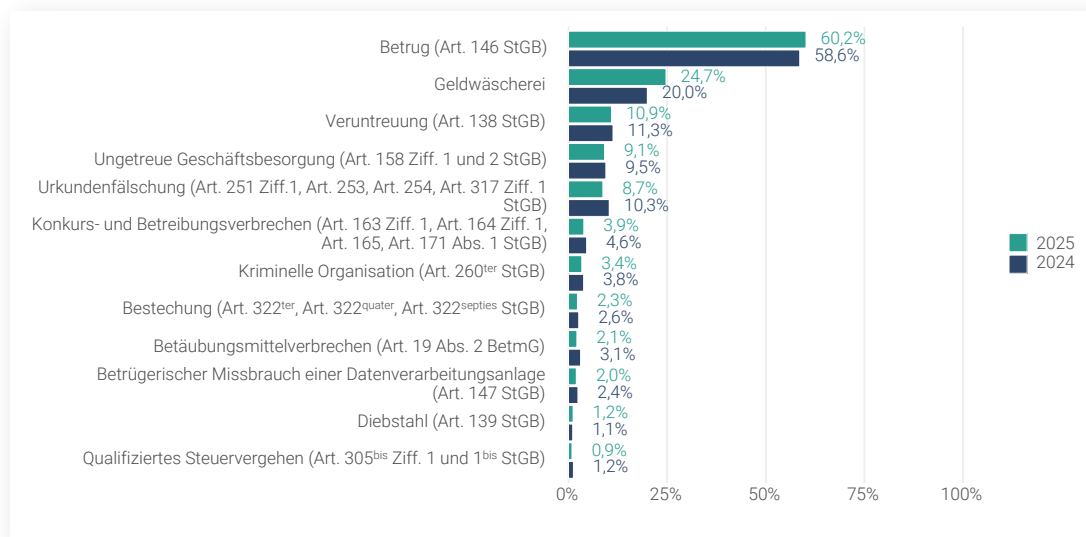
²⁴ Finanzintermediäre können im Informationssystem goAML mehrere verdachtsauslösende Elemente für ihre Meldungen angeben. Hingegen ist es nicht mehr möglich, einen aussagekräftigen Vergleich mit den Zahlen der Jahre vor 2020 vorzunehmen.

die Bundesanwaltschaft. Wie in den Vorjahren konzentrierte sich mehr als die Hälfte der Anzeigen auf einige wenige kantonale Staatsanwaltschaften. Anzeigen an die Staatsanwaltschaften der Kantone Zürich (15,1%), Waadt (12,7%) und Genf (9,7%) sowie an die Bundesanwaltschaft (9,5%) machen zusammen knapp die Hälfte aller von der MROS übermittelten Anzeigen aus (vgl. Tabelle 2).

Tabelle 2: Übermittelte Anzeigen nach Strafverfolgungsbehörden 2020 – 2025

Behörde	2020	2021	2022	2023	2024	2025	2025 in absoluten Zahlen	Durchschnitt 2020 – 2025
Zürich	18,9%	21,1%	20,4%	16,3%	17,9%	15,1%	208	18,3%
Waadt	11,1%	11,6%	10,6%	8,3%	12,4%	12,7%	175	11,1%
Genf	11,5%	11,3%	11,6%	17,6%	10,2%	9,7%	134	12,0%
Bundesanwaltschaft	9,0%	9,1%	6,4%	13,0%	10,3%	9,5%	130	9,6%
Aargau	5,3%	5,2%	6,7%	4,2%	5,7%	8,1%	111	5,9%
Bern	7,5%	6,7%	6,9%	6,5%	7,7%	7,3%	100	7,1%
Freiburg	2,7%	3,1%	2,1%	1,3%	2,1%	4,1%	57	2,6%
St. Gallen	3,5%	4,0%	6,3%	5,3%	5,3%	4,1%	57	4,8%
Solothurn	1,9%	2,0%	2,1%	1,4%	2,1%	3,5%	48	2,2%
Tessin	5,0%	4,8%	3,6%	4,6%	5,5%	3,4%	47	4,5%
Luzern	3,5%	2,9%	2,6%	2,5%	3,9%	3,3%	45	3,1%
Basel-Landschaft	2,1%	1,7%	2,3%	1,8%	2,2%	2,8%	39	2,1%
Thurgau	3,0%	2,1%	2,6%	3,2%	1,7%	2,8%	39	2,6%
Wallis	2,7%	2,4%	3,0%	2,2%	2,9%	2,7%	37	2,6%
Basel-Stadt	2,6%	2,3%	2,3%	1,8%	3,2%	2,1%	29	2,4%
Neuenburg	2,3%	1,9%	1,7%	1,3%	1,0%	2,0%	28	1,7%
Zug	2,5%	2,6%	2,2%	2,2%	1,2%	1,4%	19	2,0%
Schwyz	1,0%	1,1%	1,9%	2,1%	1,5%	1,0%	14	1,4%
Appenzell Ausserrhoden	0,6%	0,8%	1,3%	0,9%	0,5%	0,7%	10	0,8%
Graubünden	1,5%	1,0%	1,1%	0,6%	1,1%	0,7%	9	1,0%
Jura	0,3%	1,0%	0,2%	0,7%	0,4%	0,7%	9	0,5%
Nidwalden	0,3%	0,4%	0,6%	0,6%	0,3%	0,6%	8	0,5%
Schaffhausen	0,5%	0,5%	0,6%	0,7%	0,6%	0,6%	8	0,6%
Obwalden	0,2%	0,1%	0,2%	0,0%	0,2%	0,4%	5	0,2%
Glarus	0,2%	0,1%	0,4%	0,6%	0,2%	0,3%	4	0,3%
Uri	0,3%	0,1%	0,2%	0,1%	0,0%	0,3%	4	0,2%
Appenzell Innerrhoden	0,0%	0,1%	0,2%	0,2%	0,3%	0,1%	1	0,2%
Total	100,0%	100,0%	100,0%	100,0%	100%	100%	1375	100%

Abbildung 7: Häufigkeit der angezeigten Straftatbestände an die Strafverfolgungsbehörden, 2024 – 2025, Häufigkeitsauswahl, Nennungen in % an Total aller Meldungen (Mehrfachnennungen möglich)



Im Berichtsjahr 2025 übermittelte die MROS am häufigsten Anzeigen an die Strafverfolgungsbehörden, die mutmasslich Betrug als Vortat betrafen, entweder als alleinige Straftat oder in Kombination mit weiteren Delikten (60,2%, vgl. Abbildung 7). Bei rund jeder zehnten der 1375 Anzeigen an die Strafverfolgungsbehörden bestand ein begründeter Verdacht auf Veruntreuung (10,9%) und/oder ungetreue Geschäftsbesorgung (9,1%). In rund einem Viertel der Übermittlungen an eine Strafverfolgungsbehörde zeigte die MROS den Straftatbestand der Geldwäscherei als solchen an. Dies war insbesondere in Konstellationen der Fall, in denen die beschuldigte Person der Vortat nicht mit jener Person identisch war, welche die geldwäschereirelevanten Handlungen vorgenommen hatte.

3.8 Rückmeldungen der Strafbehörden

Gestützt auf Artikel 29a GwG sind die Strafbehörden verpflichtet, der MROS Informationen über hängige Verfahren, insbesondere in den Bereichen Geldwäscherei, kriminelle und terroristische Organisationen sowie Terrorismusfinanzierung zu übermitteln.²⁵ Zudem informieren sie die MROS

über Verfügungen, die sie infolge einer Anzeige der Meldestelle erlassen haben.²⁶ Diese Rückmeldungen bilden eine zentrale Grundlage für die MROS im Rahmen der Unterstützung der Strafverfolgungsbehörden.

Die Statistik des Jahresberichts 2024 zeigte, dass der MROS bei einem erheblichen Teil der übermittelten Anzeigen noch keine Rückmeldungen zum Verfahrensstand vorlagen. Dies ist unter anderem auf die Dauer der strafprozessualen Verfahren zurückzuführen.²⁷ Per 31. Dezember 2024 verfügte die MROS lediglich bei 35,7% der zwischen 2020 und 2023 übermittelten Fälle über Informationen zum Stand des Verfahrens. Im Berichtsjahr setzte die MROS ihre Bemühungen fort, den Anteil ausstehender Rückmeldungen zu verringern, und suchte den Austausch mit den Strafbehörden, um die gemäss Artikel 29a GwG vorgesehenen Informationen zu erhalten. In der Folge konnte der Informationsstand der MROS zum Verfahrensstatus der übermittelten Fälle erhöht werden: Für den Zeitraum 2020 bis 2023 lagen der MROS am 31. Dezember 2025 nun in jedem zweiten Fall Angaben zum Stand des Verfahrens vor (49,7%). Wer-

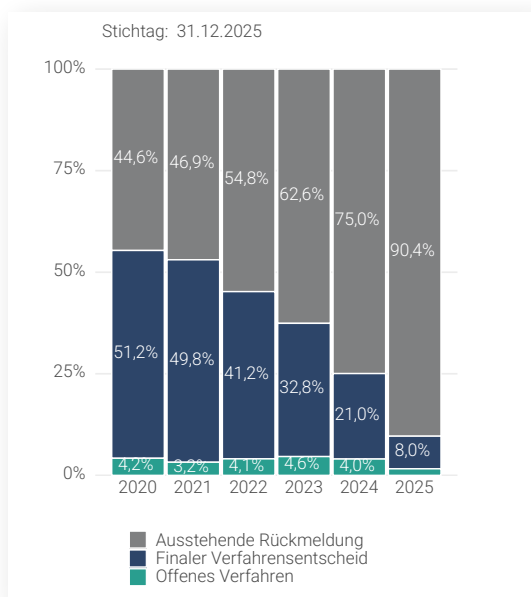
²⁵ Art. 29a Abs. 1 GwG: Die Strafbehörden melden der Meldestelle umgehend sämtliche hängigen Verfahren im Zusammenhang mit den Art. 260^{ter}, 260^{quinquies} Abs. 1, 305^{bis} und 305^{ter} Abs. 1 StGB. Sie stellen ihr rasch Urteile und Einstellungsverfügungen inklusive Begründung zu.

²⁶ Art. 29a Abs. 2 GwG.

²⁷ Vgl. [Jahresbericht MROS 2024](#), S. 22.

den – in Übereinstimmung mit der Methodik des Jahresberichts 2024 – die Übermittlungen derjenigen drei Jahre berücksichtigt, die zum Stichtag 31. Dezember 2025 mindestens zwölf Monate zurücklagen (2021 – 2024), betrug die Rückmeldequote im Jahr 2025 46,6%.

Abbildung 8: Rückmeldungen und Stand der im jeweiligen Jahr übermittelten Anzeigen am Stichtag 31. Dezember 2020 – 2025



3.9 Terrorismusfinanzierung

Im Berichtsjahr 2025 gingen bei der MROS insgesamt 114 Meldungen wegen Verdachts auf Terrorismusfinanzierung ein. Dies entspricht einem Anteil von 0,5% aller im Jahr 2025 eingegangener Verdachtsmeldungen. In der Mehrzahl der Fälle wurden diese Meldungen zusätzlich mit weiteren mutmasslichen Vortaten in Verbindung gebracht. Am häufigsten wurden dabei folgende Delikte genannt:

- Zugehörigkeit zu kriminellen und terroristischen Organisationen²⁸ (31 Nennungen)
- Betrug²⁹ (16 Nennungen)

- Bestechung (7 Nennungen)
- Verstoss gegen das Embargogesetz³⁰ (5 Nennungen)
- Verstoss gegen das Betäubungsmittelgesetz³¹ (4 Nennungen)
- Urkundenfälschung (4 Nennungen)³²

Die Meldungen mit Verdacht auf Terrorismusfinanzierung stammen überwiegend von Banken (94 Meldungen), gefolgt von den Zahlungsverkehrsdienstleistern (9 Meldungen).

Als Verdachtsauslöser für die Meldung nennen die Finanzintermediäre 2025 am häufigsten:

- Medienberichte (32 Nennungen)
- Informationen von Dritten (29 Nennungen)
- Transaktionsmonitoring (24 Nennungen)
- Bartransaktionen (19 Nennungen)
- Unklarheiten bezüglich wirtschaftlichen Hintergrunds (17 Nennungen)

Wie in den Vorjahren zeigt sich damit, dass Verdachtsmeldungen im Bereich der Terrorismusfinanzierung häufig durch Medienberichte ausgelöst wurden. Die 114 im Verlauf des Jahres 2025 eingegangenen Meldungen führten bis 31. Dezember 2025 zu fünf Anzeigen zuhanden der zuständigen Strafverfolgungsbehörden.

3.10 Organisierte Kriminalität

Von den im Jahr 2025 bei der MROS eingegangenen rund 21 000 Verdachtsmeldungen gaben die Finanzintermediäre in 695 Fällen (3,3%) einen möglichen Zusammenhang mit kriminellen Organisationen an. Die überwiegende Mehrheit dieser Verdachtsmeldungen stammte von Finanzintermediären aus dem Bankensektor (77,8%), gefolgt von Zahlungsdienstleistern mit 17,7%. Auslöser für die Verdachtsmeldung waren nach Angaben der Finanzintermediäre in einem Drittel der Fälle «Diverses» (33,7%). Spezifisch nannten sie hauptsächlich Informationen aus Medien (25,3%), Bartransaktionen (21,6%) und/oder einem Transaktionsmonitoring (17,1%; vgl. Tabelle 3).

²⁸ Art. 260^{ter} StGB.

²⁹ Art. 146 StGB.

³⁰ Art. 9 Abs. 2 Bundesgesetz über die Durchsetzung von internationalen Sanktionen (Embargogesetz, EmbG), SR 946.231.

³¹ Art. 19 Abs. 2 Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelgesetz, BetmG), SR 812.121.

³² Art. 251 Ziff.1, Art. 253, Art. 254, Art. 317 Ziff. 1 StGB.

Tabelle 3: Häufigkeit verdachtsauslösender Merkmale in Meldungen wegen mutmasslichen Verbindungen zu kriminellen Organisationen

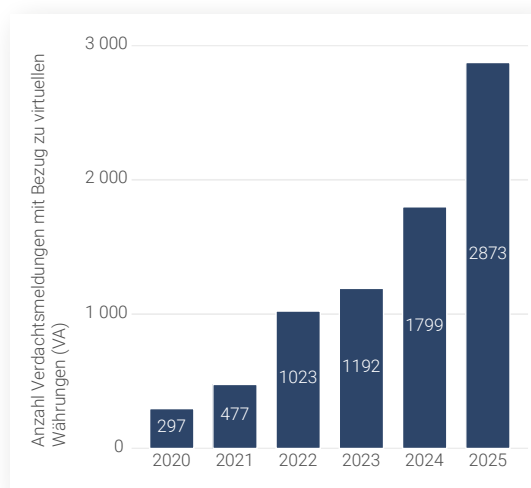
Verdachtsauslöser (Mehrfachnennungen möglich, Häufigkeitsauswahl)	Anzahl Nennungen	in % an Total aller Meldungen
Diverse	234	33,7%
Medien	176	25,3%
Bartransaktion	150	21,6%
Transaktionsmonitoring	119	17,1%
Wirtsch. Hintergrund unklar	42	6,0%
Eröffnung Geschäftsbeziehung	38	5,5%
Information Dritte	36	5,0%
Information SVB	35	8,0%
Durchlaufkonten	25	6,8%
Kreditgeschäft	23	4,7%

Zusätzlich zur vermuteten Verbindung zu einer kriminellen Organisation nannten die Finanzintermediäre als weitere mögliche Vortat häufig Betrug (53,5%) und/oder Urkundenfälschung (17,4%). Die 695 Verdachtsmeldungen im Berichtsjahr mit einem möglichen Zusammenhang zu kriminellen Organisationen führten zu 32 Anzeigen bei den zuständigen Strafverfolgungsbehörden.

3.11 Verdachtsmeldungen mit Bezug zu virtuellen Währungen

Die MROS identifizierte im Berichtsjahr 2025 2873 Verdachtsmeldungen mit Bezug zu virtuellen Währungen (Virtual Assets [VA]³³; vgl. Abbildung 9). Gegenüber dem Vorjahr entspricht dies einer Zunahme von 59,7%.³⁴ Diese Entwicklung stellt die MROS vor zunehmende Herausforderungen: Virtuelle Währungen erschweren die Nachverfolgung von Geldströmen und damit die Herkunft des Vermögens sowie die eindeutige Identifikation des wirtschaftlich Berechtigten. Wie der im ersten Quartal 2024 publizierte Bericht «National Risk

Assessment (NRA) – Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets» vertieft darlegt, bringen Kryptowährungen erhöhte Risiken.³⁵

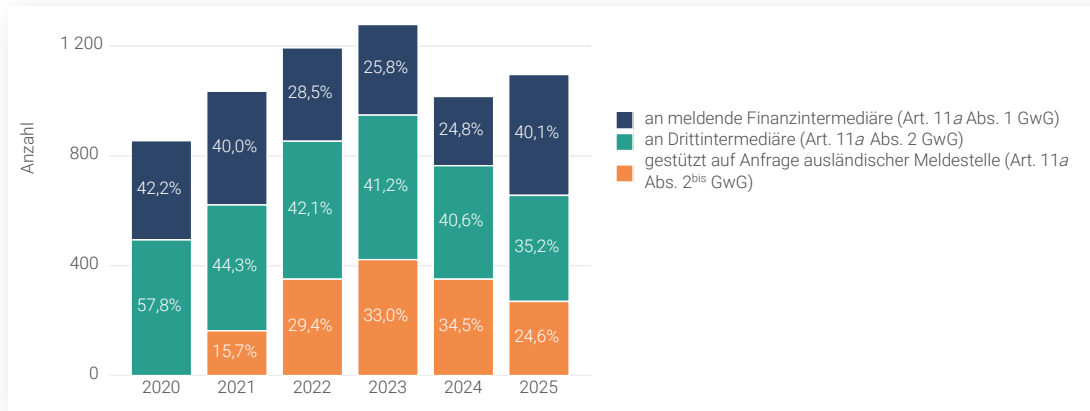
Abbildung 9: Anzahl Meldungen mit einem Bezug zu virtuellen Währungen (VA), 2020 – 2025

³³ Mit der Verankerung von Art. 4 Abs. 2 Bst. a in der Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung, GwV), SR 955.01, am 1. Januar 2016 wurde in der Schweiz der Begriff der «virtuellen Währung» erstmals in einem rechtlichen Erlass erfasst.

³⁴ Inwiefern in einer Meldung Transaktionen mit virtuellen Währung Gegenstand des Verdachts sind, lässt sich bis anhin nicht direkt erfassen, da solche Transaktionen nicht eindeutig identifizierbar sind. Verdachtsmeldungen mit einem relevanten VA-Bezug wurden deshalb einerseits mittels Transaktionen zwischen den in der Meldung angezeigten Konten und Konten von schweizerischen oder ausländischen Finanzintermediären mit VASP-Tätigkeit und andererseits mit einer Schlagwortliste relevanter Begriffe identifiziert. Es ist deshalb anzunehmen, dass die Bedeutung von Kryptowährungen in Verdachtsmeldungen eher unterschätzt wird.

³⁵ National Risk Assessment (NRA) – Bericht Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, Januar 2024.

Abbildung 10: Aufforderung zur Herausgabe von Informationen nach Artikel 11a GwG
2020 – 2025



Seit Frühjahr 2024 erfasst die MROS Finanzintermediäre, deren Haupttätigkeit im Bereich virtuelle Vermögenswerte liegt, als eigene Kategorie.³⁶ Damit sind Aussagen über das Meldeverhalten dieser Kategorie von Finanzintermediären möglich (vgl. Tabelle 1). Bis zum 31. Dezember 2025 registrierten sich 49 Finanzintermediäre in der Kategorie VASP/FinTech in goAML.

3.12 Herausgabe von Informationen nach Artikel 11a GwG

2025 richtete die MROS gestützt auf Artikel 11a GwG insgesamt 1096 Informationsanfragen an Finanzintermediäre. Gegenüber dem Vorjahr entspricht dies einer Zunahme von 7,9% (2024: 1016). Nachdem die Anzahl der Anfragen im Jahr 2024 erstmals seit 2020 rückläufig gewesen war, nahm sie im Berichtsjahr erneut leicht zu.

Im Unterschied zu den Jahren 2020 bis 2024 richtete die MROS 2025 wieder häufiger Anfragen an meldende Finanzintermediäre und weniger an so-

genannte Drittintermediäre: 40,1% der Informationsanfragen gingen an die Finanzintermediäre der ursprünglichen Verdachtsmeldungen (+15,3%, Art. 11a Abs. 1 GwG³⁷, vgl. Abbildung 10) und 35,2% an Drittintermediäre (-5,4%, Art. 11a Abs. 2 GwG³⁸), die neben dem meldenden Finanzintermediär an einer Transaktion oder einer Geschäftsbeziehung beteiligt sind oder waren.

Rund jede vierte Anfrage um Informationen richtete die MROS dagegen gestützt auf die Analyse von Informationen einer ausländischen Meldestelle an einen Finanzintermediär (24,6%, Art. 11a Abs. 2^{bis} GwG³⁹). Erstmals seit der Einführung von Artikel 11a Absatz 2^{bis} GwG im Jahr 2021 nahm der Anteil dieser Anfragen gegenüber den anderen Anfragen nach Artikel 11a GwG wieder ab. (-9,9% gegenüber Vorjahr).

Informationsanfragen nach Artikel 11a GwG bilden einen integralen Bestandteil der vertieften Analyse der MROS und erfolgen im Vorfeld einer allfälligen Übermittlung an die Strafverfolgungsbehörden.

³⁶ Im März 2024 wurden die in goAML registrierten Finanzintermediäre gebeten, der MROS zu melden, falls sie aufgrund ihrer Haupttätigkeit in die Kategorie eines VASP fallen.

³⁷ Art. 11a Abs. 1 GwG: Benötigt die Meldestelle zusätzliche Informationen für die Analyse einer bei ihr nach Art. 9 GwG oder nach Art 305^{ter} Absatz 2 StGB eingegangenen Meldung, so muss ihr der meldende Finanzintermediär diese auf Aufforderung hin herausgeben, soweit sie bei ihm vorhanden sind.

³⁸ Art. 11a Abs. 2 GwG: Wird aufgrund dieser Analyse erkennbar, dass neben dem meldenden Finanzintermediär weitere Finanzintermediäre an einer Transaktion oder Geschäftsbeziehung beteiligt sind oder waren, so müssen die beteiligten Finanzintermediäre der Meldestelle auf Aufforderung hin alle damit zusammenhängenden Informationen herausgeben, soweit sie bei ihnen vorhanden sind.

³⁹ Art. 11a Abs. 2^{bis} GwG: Wird aufgrund der Analyse von Informationen, die von einer ausländischen Meldestelle stammen, erkennbar, dass diesem Gesetz unterstellte Finanzintermediäre an einer Transaktion oder Geschäftsbeziehung im Zusammenhang mit diesen Informationen beteiligt sind oder waren, so müssen die beteiligten Finanzintermediäre der Meldestelle auf Aufforderung hin alle damit zusammenhängenden Informationen herausgeben, soweit sie bei ihnen vorhanden sind.

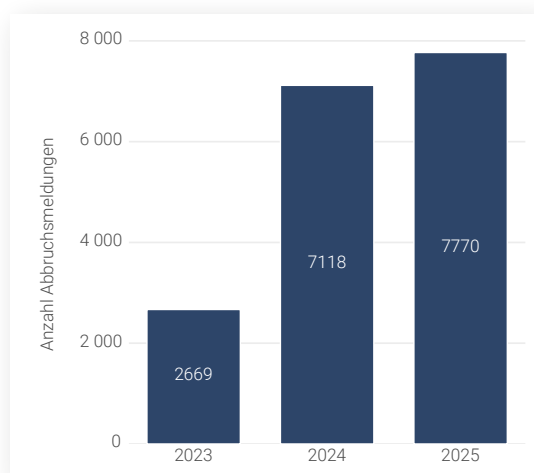
2025 stützte sich jede fünfte Anzeige, welche die MROS an eine Strafverfolgungsbehörde übermittelte, auf Informationen und Erkenntnisse aus solchen Anfragen (2025: 20,1%). In Abhängigkeit von der Komplexität des jeweiligen Falls flossen dabei in einzelne Anzeigen Informationen aus mehreren, an unterschiedliche Finanzintermediäre gerichtete Informationsanfragen ein.

3.13 Abbruchmeldungen nach Artikel 9b GwG

Gestützt auf Artikel 9b GwG⁴⁰ können Finanzintermediäre seit dem 1. Januar 2023 eine Geschäftsbeziehung nach 40 Arbeitstagen nach deren Meldung an die MROS beenden, sofern sie bis dahin nicht über eine Übermittlung an die Strafverfolgungsbehörden informiert wurden. Den Abbruch der Geschäftsbeziehung hat der Finanzintermediär der MROS unmittelbar zu melden.⁴¹

Nach dem im Jahr 2024 festgestellten deutlichen Anstieg hat sich die Zunahme der Abbruchmeldungen im Berichtsjahr 2025 verflacht: Die MROS erhielt 7770 Abbruchmeldungen und damit +9,2% mehr als im Vorjahr (vgl. Abbildung 11). 7,6% der Ab-

Abbildung 11: Anzahl Abbruchmeldungen
2023 – 2025



bruchmeldungen betrafen Verdachtsmeldungen, die über den Jahresverlauf 2025 an die Strafverfolgungsbehörden weitergeleitet wurden.

Seit Herbst 2025 können Finanzintermediäre unter bestimmten Voraussetzungen⁴² direkt mit der Verdachtsmeldung der MROS ihre Absicht mitteilen, die gemeldete Geschäftsbeziehung nach Ablauf der Frist von 40 Arbeitstagen abbrechen. 1462 Verdachtsmeldungen enthielten einen solchen Hinweis.

3.14 Informationsaustausch mit ausländischen FIUs

Der Informationsaustausch zwischen der MROS und ausländischen FIUs erfolgt im Rahmen der Amtshilfe und bildet ein zentrales Instrument bei der Bekämpfung von Geldwäscherei und deren Vortaten, der Terrorismusfinanzierung sowie der organisierten Kriminalität. Für die Analysearbeit der MROS sind diese Informationen von wesentlicher Bedeutung, da ein erheblicher Teil der von Schweizer Finanzintermediären eingereichten Verdachtsmeldungen einen Auslandsbezug aufweist.⁴³

Im Berichtsjahr 2025 richtete die MROS 237 Auskunftersuchen an ausländische FIUs. Gegenüber dem Vorjahr entspricht dies einem leichten Rückgang von 0,8%. Umgekehrt gingen bei der MROS über den Jahresverlauf 660 Anfragen von 91 ausländischen Meldestellen ein (-15,1% im Vergleich zum Vorjahr). Die MROS bearbeitete 323 der eingegangenen Anfragen sowie zusätzlich 99 Anfragen aus dem Vorjahr.

An Bedeutung gewonnen hat hingegen der spontane Informationsaustausch zwischen der MROS und ausländischen FIUs. Ausländische FIUs und die MROS können ohne vorherige Anfrage Informationen austauschen, sei es aus dem Ausland mit einem Bezug zur Schweiz oder von der MROS an eine ausländische FIU. 2025 erhielt die MROS 932 Spontaninformationen aus 56 Ländern. Damit er-

⁴⁰ Nach Art. 9b GwG können Finanzintermediäre eine nach Art. 9 Abs. 1 Bst. a GwG oder nach Art. 305^{ter} Abs. 2 StGB gemeldete Geschäftsbeziehung abbrechen, sofern die Meldestelle nicht dem Finanzintermediär innert 40 Arbeitstagen mitteilt, dass sie die gemeldeten Informationen einer Strafverfolgungsbehörde übermitteln hat.

⁴¹ Art. 9b Abs. 3 GwG.

⁴² Siehe Kapitel 5.1.

⁴³ [Zweite nationale Risikoanalyse \(NRA\) – Bericht über die nationale Beurteilung der Geldwäscherei und Terrorismusfinanzierungsrisiken in der Schweiz](#), Oktober 2021.

hielt die MROS 2025 24,1% mehr solcher Spontaninformationen aus dem Ausland als im Vorjahr (2024: 751 aus 45 Ländern). Die MROS wiederum versendete 223 Spontaninformationen an 53 ausländische FIUs und damit 6,6% mehr als 2024 (2024: 189 an 41 FIUs).

3.15 Informationsaustausch mit Schweizer Behörden

Gestützt auf Artikel 29 GwG teilt die MROS mit Schweizer Behörden relevante Informationen auf Anfrage oder spontan. Es handelt sich um Aufsichtsbehörden oder andere Behörden, die im Kampf gegen die Geldwäscherei und deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung aktiv sind.⁴⁴ Im Berichtsjahr 2025 erhielt die MROS 498 Informationsanfragen von 46 Schweizer Behörden zu bestimmten Bankkonten, Personen oder Unternehmen (+11,4%; 2024: 447). Knapp drei von vier Anfragen stammten von polizeilichen Behörden. Die MROS stellte umgekehrt 47 Anfragen an 15 Schweizer Behörden. In 490 Fällen übermittelte die MROS unaufgefordert Informationen an Schweizer Aufsichts- und andere Behörden (+36,9%; 2024: 358).⁴⁵ 2025 gingen zudem 120 Spontaninformationen von inländischen Behörden bei der MROS ein (13,2%, 2024: 106).

⁴⁴ In den Zahlen nicht erfasst, sind die Informationsanfragen der MROS im Zuge ihrer Analysen bei anderen Bundes-, Kantons- und Gemeindebehörden.

⁴⁵ Zudem übermittelte die MROS in 72 Fällen zusätzliche Informationen an die Strafverfolgung, nachdem bereits eine Anzeige erfolgt war.

4 Trends

Das Kapitel «Trends» im Jahresbericht 2025 setzt die im Vorjahr begonnene Neuausrichtung fort und ersetzt weiterhin das frühere Kapitel «Typologien». Die Typologien werden seit Mai 2025 auf der Homepage der MROS publiziert. Die Trendanalysen ermöglichen eine verdichtete und themenübergreifende Sicht auf aktuelle Feststellungen der MROS und tragen zur Einordnung relevanter Entwicklungen im Bereich der Geldwäscherei und der Terrorismusfinanzierung bei. Im Berichtsjahr 2025 stehen drei Phänomene im Fokus, die sich durch eine hohe Dynamik, zunehmende Internationalisierung und besondere Herausforderungen für die Finanzintermediäre auszeichnen: Betrug durch manipulierte Geschäftskommunikation als weiterhin stark verbreitete Form des Betrugs mit hohem Schadenspotenzial, sogenannte Schattenflotten im Zusammenhang mit der Umgehung von Sanktionen sowie Aktivitäten der italienischen Mafia, deren Strukturen und Finanzströme auch für den Schweizer Finanzplatz von Bedeutung sind.

4.1 Betrug durch manipulierte Geschäftskommunikation

Betrug mittels fingierter Geschäftskommunikation stellt in der Schweiz eine etablierte und zunehmend professionalisierte Betrugsform dar. Die dadurch erreichten Vermögensschäden erreichen regelmässig Millionenbeträge. Die Täterschaften agieren arbeitsteilig und mit erheblichem Vorbereitungsaufwand, wodurch auch erfahrene und fachlich qualifizierte Mitarbeitende betroffen sein können.

Der Modus Operandi ist komplex und strategisch geplant. Die Täterschaft analysiert über einen längeren Zeitraum interne Strukturen von Unternehmen, einschliesslich Entscheidungsprozessen, Kommunikationswegen und Hierarchien. Hierzu werden häufig öffentlich zugängliche Informationen wie Geschäftsberichte, Handelsregistereinträge oder Inhalte aus sozialen Netzwerken genutzt. In einem weiteren Schritt wird die Identität einer Führungsperson oder eines Geschäftspartners nachgeahmt oder kompromittiert. Dies erfolgt entweder durch den Einsatz von Spoofing-Techniken oder durch den Zugriff auf legitime E-Mail-Konten. Die betroffenen Mitarbeitenden erhalten so täuschend echt formulierte Zahlungsanweisungen, die als ordentliche geschäftliche Transaktionen erscheinen. Die veranlassten Überweisungen erfol-

gen jedoch auf Konten, die von der Täterschaft kontrolliert werden. Die Schweiz ist aufgrund ihrer stark international vernetzten Wirtschaftsstruktur, insbesondere im Bereich kleiner und mittlerer Unternehmen, ein besonders attraktives Ziel solcher Betrugshandlungen. Schlanke Organisationsformen, klare Hierarchien und ein traditionell hohes Vertrauen in interne Kommunikation begünstigen den Erfolg dieser Täuschungen. Zudem erschwert die Mehrsprachigkeit die Erkennung subtiler sprachlicher Unstimmigkeiten in E-Mails.

Aus Sicht der MROS zeigen sich in diesem Zusammenhang zwei typische Melde- und Informationsflüsse: Einerseits gehen Verdachtsmeldungen ein, welche die mutmasslichen Täterkonten identifizieren oder Anfragen nationaler Strafverfolgungsbehörden, die ihrerseits Informationen von ausländischen FIUs benötigen. Andererseits treffen dringliche Ersuchen ausländischer FIUs ein, mit dem Ziel, Transaktionen unverzüglich zu blockieren oder Konten zu sperren. In diesen Fällen ist zeitnahes Handeln von zentraler Bedeutung: Jede Verzögerung – insbesondere durch mehrstufige Zuständigkeitswege der involvierten Behörden – kann dazu führen, dass Gelder rasch ins Ausland weitergeleitet oder in Bargeld umgewandelt werden.

Im Zusammenhang mit solchen Betrugsfällen bestehen positive Erfahrungen mit dem internationalen FIU-Netzwerk. Auch wenn Meldungen häufig erst nach Ausführung der Transaktion eingehen, stellen ausländische FIUs in der Regel rasch alle erforderlichen Informationen für weiterführende Massnahmen (z. B. ein nachfolgendes Rechtshilfersuchen) zur Verfügung. In einzelnen Fällen gelingt es sogar, die notwendigen Schritte einzuleiten, bevor die Gelder über Korrespondenzbanken beim ausländischen Institut eintreffen. Durch eine effiziente Zusammenarbeit zwischen Geschädigten, Strafverfolgungsbehörden, FIUs und involvierten Banken ist es in solchen Konstellationen möglich, eingehende Gelder unmittelbar zu blockieren.

Ein aktuelles Beispiel betrifft einen Fall von Business-E-Mail-Compromise (sog. BMC-Betrug): Ein Schweizer Unternehmen unterhielt eine laufende Geschäftsbeziehung mit einem Unternehmen in den Vereinigten Arabischen Emiraten. Vor diesem Hintergrund erschien eine per E-Mail eingegangene

Rechnung über mehrere Millionen Schweizer Franken zunächst plausibel. Erst nach der Überweisung wurde der Betrug erkannt. Die Zahlung gelangte daher nicht an den legitimen Geschäftspartner, sondern auf ein von der Täterschaft kontrolliertes ausländisches Konto.

Die Geschädigten nahmen mit der Bank umgehend Kontakt auf, um die bereits ausgeführte Transaktion zu stoppen. Parallel dazu erfolgte durch die zuständige Polizei eine Anfrage bei der MROS mit der Bitte um sofortige Blockierung der Transaktion durch die FIU der Vereinigten Arabischen Emirate. Diese verfügt seit Inkrafttreten des *Federal Decree-Law No. 10 (2025)* über erweiterte Befugnisse im Bereich der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung. Der Leiter der FIU kann Transaktionen bis zu 10 Arbeitstage suspendieren («suspension power») und Gelder bzw. fondsbezogene Vermögenswerte bis zu 30 Tage einfrieren («freezing power»). Schlussendlich konnten eine Einzahlung auf das Konto in den Vereinigten Arabischen Emiraten verhindert werden. Wären die Gelder auf dem Konto der Täterschaft eingegangen, wären die Gelder auf Grund der sehr guten und umgehenden, nationalen und internationalen Zusammenarbeit umgehend blockiert worden.

Im internationalen Vergleich ist festzustellen, dass die MROS per Stand heute – im Gegensatz zu zahlreichen ausländischen FIUs – über keine eigenständigen gesetzlichen Befugnisse zur Suspendierung von Transaktionen oder zur Sperrung von Konten verfügt. Entsprechende Kompetenzen bestehen unter anderem in Belgien, Italien, Frankreich, den Niederlanden, Luxemburg, Spanien und Portugal. Auf europäischer Ebene verpflichtet die EU-Richtlinie (EU) 2024/1640 vom 31. Mai 2024 sämtliche FIUs der Europäischen Union, spätestens ab dem 10. Juli 2027 über systematische Befugnisse zur Aussetzung von Transaktionen und zur Blockierung von Konten zu verfügen. Diese Kompetenzen sollen nicht nur bei Verdacht auf Geldwäscherei oder Terrorismusfinanzierung, sondern auch im Rahmen rein analytischer Tätigkeiten zur Anwendung kommen können.⁴⁶ International ist eine vergleichbare Entwicklung zu beobachten:

Immer mehr FIUs erhalten weitreichende Eingriffsbefugnisse zur sofortigen Sicherung mutmasslich deliktischer Vermögenswerte.

4.2 Schattenflotten

In den vergangenen Jahren ist das Phänomen verstärkt in den Fokus der öffentlichen Berichterstattung gerückt. Unter dem Begriff «Schattenflotten» werden Schiffe oder ganze Flotten verstanden, die bewusst ausserhalb etablierter Kontroll-, Transparenz- und Überwachungsmechanismen operieren, um insbesondere internationale Sanktionen zu umgehen. Häufig handelt es sich um ältere, nicht mehr zertifizierte Tanker oder Frachtschiffe. Durch widersprüchliche oder häufig wechselnde Schiffs- und Registrierungsdaten⁴⁷ sowie durch komplexe, intransparente Eigentümerstrukturen⁴⁸ wird versucht, sowohl die Herkunft und den Bestimmungsort der transportierten Güter als auch die wirtschaftlich Berechtigten effektiv zu verschleiern.

Obwohl die Schweiz als Binnenstaat – abgesehen vom Zugang zur Nordsee über den Rhein – über keine direkte maritime Anbindung verfügt, ist sie von diesem Phänomen in mehrfacher Hinsicht betroffen. Als international bedeutender Finanzplatz beherbergt die Schweiz einen grossen Rohstoffhandelssektor sowie wichtige Versicherungs- und Logistikunternehmen. Zudem sind mehrere der weltweit grössten Schifffahrtsunternehmen in der Schweiz domiziliert. Das schweizerische Seeschiffsregister in Basel fungiert darüber hinaus als Registerstaat für zahlreiche Passagier- und Kreuzfahrtschiffe auf europäischen Binnenwasserstrassen. Vor diesem Hintergrund kommt der Auseinandersetzung mit Schattenflotten im Kontext der Sanktionsumgehung – insbesondere im Zusammenhang mit der militärischen Aggression Russlands gegen die Ukraine – auch aus Sicht der MROS eine erhöhte Bedeutung zu.

Wie bereits im Jahresbericht 2022 dargelegt liegt die Zuständigkeit für das schweizerische Sanktionsrecht beim Staatssekretariat für Wirtschaft (SECO), welches auch den Vollzug der entsprechenden

⁴⁶ Art. 24 der Richtlinie (EU) 2024/1640.

⁴⁷ Die Schiffe fahren meist unter so genannten Billigflaggen wie Panama, Marshallinseln oder Liberia.

⁴⁸ Oft über undurchsichtige Sitzgesellschaften und Offshore-Firmen.

Meldepflichten nach Schweizer Sanktionsrecht überwacht. In Fällen potenziell schwerwiegender Verstösse gegen das Embargogesetz kann jedoch eine Meldung eines Schweizer Finanzintermediärs an die MROS angezeigt sein. Dies, sofern im Zuge der Abklärungen zur Verletzung oder Umgehung von Sanktionen Anhaltspunkte für Geldwäscherei oder Terrorismusfinanzierung auftreten.⁴⁹

Schattenflotten sind kein neues Phänomen, das erst im Zusammenhang mit dem Angriff Russlands auf die Ukraine entstanden ist. Bereits in den 1920er-Jahren wurden US-Tanker unter panamaischer Flagge eingesetzt, um Alkohol transportieren zu können. In späteren Jahrzehnten nutzten unter anderem Nordkorea und Iran entsprechende Strukturen, um trotz internationaler Sanktionen Waren ein- oder auszuführen. Die aktuelle sicherheitspolitische Lage hat jedoch zu einer deutlichen Intensivierung und Professionalisierung solcher Praktiken geführt.

Auch aus Sicht der MROS zeigt sich, dass das Thema Schattenflotten für den Schweizer Finanzplatz relevant ist. Einerseits haben Schweizer Finanzintermediäre entsprechende Verdachtsmeldungen eingereicht, andererseits gingen Anfragen ausländischer FIU im Zusammenhang mit mutmasslicher Sanktionsumgehung ein. Nach Informationen der MROS lassen sich verschiedene Indikatoren identifizieren, die – einzeln oder in Kombination – auf eine mögliche Sanktionsumgehung hindeuten können:

a. Schiffsdaten & Technik

- Die betroffenen Schiffe weisen ein hohes Alter auf,
- Ausflagungen erfolgen in kurzen zeitlichen Abständen,
- Wartungs- und Sicherheitszertifikate erscheinen unvollständig, ungewöhnlich oder inkonsistent.

b. Eigentümer- und Betreiberstruktur

- Die Eigentümerstruktur ist komplex und intransparent; häufig werden Briefkastenfirmen und Offshore-Firmen eingesetzt,
- Häufige Eigentümerwechsel,

- Sitzstaaten der Eigentümergesellschaften liegen in Risikoländern, etwa aufgrund fehlender Transparenzregister,
- Die wirtschaftlich berechtigten Personen sind nicht eindeutig identifiziert und/oder werden durch undurchsichtige Konstrukte verschleiert.

c. Handels- & Routenmuster

- Die gewählten Routen erscheinen ungewöhnlich oder wirtschaftlich nicht plausibel (z. B. mit langen Umwegen),
- Es kommt zu häufigen Kursänderungen oder Stopps in Seegebieten mit bekannter Schattenflotten-Aktivität,
- Kombination von legalen und sanktionierten Destinationen.

d. Fracht- & Dokumentationslage

- Angaben zur Herkunft, Art und Menge der Ladung sind widersprüchlich oder unvollständig,
- Ursprungszertifikate oder Begleitdokumente deuten auf einen möglichen Export aus sanktionierten Staaten hin, gegebenenfalls über Drittstaaten,
- Es bestehen Diskrepanzen zwischen der deklarierten Ladung und der Grösse oder Kapazität des Schiffes.

e. Finanz- & Zahlungsstrukturen

- Zahlungsflüsse sind komplex gestaltet und erfolgen über mehrere Finanzinstitute, häufig unter Einbezug von Banken in Offshore-Zentren,
- Hinweis auf Tradebased Money Laundering (TBML), etwa durch Über- oder Unterbewertung der Ware,
- Zahlungen werden von Gesellschaften ohne erkennbare Geschäftstätigkeit ausgelöst.

f. Sanktions- und Risikobezug

- Es bestehen direkte oder indirekte Verbindungen zu sanktionierten Staaten,
- Es werden Häfen mit schwachen oder unzureichenden Kontrollen genutzt,
- Es treten bekannte High-Risk-Reedereien oder Versicherer in Erscheinung,
- Schiffe, Unternehmen oder Personen erscheinen auf Sanktions- oder Watchlists.

⁴⁹ Melderecht (Art. 305^{ter} Abs. 2 StGB) oder Meldepflicht (Art. 9 GwG).

Diese Aufzählung ist nicht abschliessend und dient der exemplarischen Veranschaulichung, welche Indikatoren Hinweise auf mögliche schwere Verstösse gegen das Embargogesetz geben und eine Verdachtsmeldung an die MROS auslösen können.

4.3 Italienische Mafia

Italienische Mafiaorganisationen sind in ein breites Spektrum krimineller Aktivitäten involviert, die sowohl klassische Deliktformen als auch moderne Erscheinungsformen der Finanz- und Wirtschaftskriminalität umfassen. Den bedeutendsten Einnahmeposten stellt nach wie vor der internationale Drogenhandel dar, der das wirtschaftliche Fundament dieser Organisationen bildet. Daneben bestehen weitere relevante Betätigungsfelder, darunter Waffenhandel, Menschenhandel sowie der Abfallhandel, der sich über ganz Italien hinaus auf Teile Osteuropas und Nordafrikas erstreckt. Hinzu kommen Korruptionsdelikte und Formen der systematischen Einflussnahme auf staatliche Strukturen und Prozesse, etwa im Zusammenhang mit öffentlichen Ausschreibungen. Parallel dazu entwickeln diese mafiösen Organisationen zunehmend Aktivitäten im Bereich moderner Wirtschaftskriminalität, einschliesslich Cyberdelikten, Anlage- und Versicherungsbetrugsfälle, betrügerische Konkursverfahren sowie Marktmanipulationen. Auch der Handel mit gefälschten Waren und Schutzgeld-erpressung – als Ausdruck territorialer Kontrolle – ergänzen dieses auf Dominanz, Einfluss und Gewinn ausgerichtete System.

Die Ermittlung verlässlicher Umsatzzahlen der italienischen Mafia ist naturgemäss schwierig. Verschiedene Studien schätzen die jährlichen Einnahmen italienischer Mafiaorganisationen auf etwa 40⁵⁰ bis 150 Milliarden⁵¹ Euro. Entsprechend hoch ist der Bedarf, diese Vermögenswerte in den legalen Wirtschaftskreislauf einzubringen und über legale Unternehmenstätigkeiten oder den Immobiliensektor zu reinvestieren.

In der Schweiz sind alle grossen italienischen Mafiaorganisationen präsent, darunter die 'Ndran-

gheta aus Kalabrien, die Camorra aus Kampanien, die Cosa Nostra sowie die apulische Sacra Corona Unita. Auch Angehörige der Criminalità barese und der Società foggiana, ebenfalls aus Apulien, sind in der Schweiz aktiv. Unter diesen Gruppen gilt die 'Ndrangheta als besonders stark in der Schweiz verankert. Die Aktivitäten der kriminellen Organisationen beschränken sich dabei nicht auf die reine Vermögensverwaltung oder Geldwäscherei. Vielmehr zielen die Organisationen darauf ab, zu infiltrieren und mittel- bis langfristig Einfluss auf wirtschaftliche und gesellschaftliche Strukturen zu nehmen. Einzelne Personen mit bekannter Nähe zu mafiösen Organisationen leben dauerhaft in der Schweiz, sind beruflich integriert und treten nach aussen unauffällig in Erscheinung. Diese soziale Einbettung stellt ein zentrales Merkmal mafiöser Strukturen dar und unterscheidet sie in ihrer Wirkungsweise von anderen Formen organisierter Kriminalität.⁵²

In der Schweiz beschränken sich die Aktivitäten der italienischen Mafia nicht auf Geldwäscherei. Zu den festgestellten Deliktsfeldern zählen unter anderem Drogenhandel, Waffenhandel, Unterstützung gesuchter Personen, Erpressung, Tötungsdelikte, Menschenhandel zu Zwecken sexueller Ausbeutung oder Arbeitsausbeutung, Lebensmittel-schmuggel, betrügerische Konkursdelikte, Anlagebetrug, Versicherungsbetrug, Falschgeldhandel sowie unerlaubtes Glücksspiel. Die Infiltration der legalen Wirtschaft erfolgt branchenübergreifend. Betroffen sind unter anderem der Immobilien- und Bausektor, Gastronomie und Lebensmittelhandel, Detailhandel, Abfallwirtschaft, Energieversorgung, Treuhandgesellschaften, Anwaltskanzleien und Notariate, Technologie- und IT-Unternehmen, Online-Gaming, Reiseagenturen, das Bestattungswesen sowie der Automobilsektor. Grundsätzlich kann jeder Wirtschaftsbereich Ziel solcher Aktivitäten werden. Der Zugang erfolgt häufig über Strohleute oder formal unauffällige Vermittler, wobei anschliessend versucht wird, Marktmechanismen und Entscheidungsprozesse zu beeinflussen.

Die MROS stellt fest, dass deliktisch erlangte Vermögenswerte in vielen Fällen bereits im Ausland in

⁵⁰ <https://aliautonomie.it/2025/01/13/legalita-cgia-le-mafie-hanno-volume-daffari-da-40-miliardi-anno-in-italia-150milia-impresenellorbita-della-criminalita/>.

⁵¹ <https://www.ilsole24ore.com/art/cosi-mafia-ha-messo-mani-cio-che-mangiamo-AEd82reG>.

⁵² <https://direzioneeinvestigativaantimafia.interno.gov.it/relazioni-semestrali/>; relazione 2024, page 341.

den legalen Finanzkreislauf eingeschleust und anschliessend über elektronische Transaktionen auf Konten in der Schweiz transferiert werden. Dabei kommen häufig Scheinrechnungen, Offshore-Gesellschaften und komplexe Zahlungsstrukturen zum Einsatz. Die Mittel werden oftmals mit legitimen Umsätzen vermischt. Zusätzlich bleibt der Einsatz von Bargeld ein relevantes Risiko, da gesetzliche Sorgfaltspflichten erst ab bestimmten Schwellenwerten greifen. Diese Rahmenbedingungen begünstigen die Nutzung von Bargeldtransaktionen durch kriminelle Organisationen, insbesondere im Zusammenhang mit Drogenhandel, Menschenhandel oder Eigentumsdelikten.

Eine weitere besondere Relevanz kommt der Rolle der Schweiz im internationalen Goldhandel und in der Goldverarbeitung zu. Die Schweiz verarbeitet einen erheblichen Anteil der weltweiten Goldproduktion. Trotz bestehender regulatorischer Vorgaben zur Importkontrolle und zur Rückverfolgbarkeit bestehen weiterhin Herausforderungen bei der lückenlosen Überprüfung der tatsächlichen Herkunft. Die Kombination aus hohen Transaktionsvolumina, globaler Vernetzung und teilweise begrenzten Kontrollmöglichkeiten kann den Sektor für den Einsatz deliktisch erlangter Vermögenswerte attraktiv machen, auch für mafiose Organisationen.⁵³

Die MROS verstärkt ihr Engagement im Kampf gegen die Geldwäscherei im Zusammenhang mit Aktivitäten krimineller Organisationen. Die Beteiligung an einer kriminellen Organisation ist gemäss Artikel 260^{ter} StGB strafbar und mit einer Freiheitsstrafe von bis zu zehn Jahren bedroht. Liegen die entsprechenden Tatbestandsmerkmale vor, handelt es sich um ein Verbrechen, das als Vortat zur Geldwäscherei in Betracht kommt. Mehrere bedeutende Fälle konnten aufgedeckt werden; diese Priorität entspricht der Strategie 2024 – 2027 von fedpol und der MROS.⁵⁴ In den vergangenen Jahren entfielen rund 5% der bei der MROS eingegangenen Verdachtsmeldungen auf Sachverhalte mit Bezug

zu kriminellen Organisationen. Die vertiefte Analyse zeigt jedoch häufig, dass die gesetzlichen Voraussetzungen von Artikel 260^{ter} StGB nicht erfüllt sind. Umgekehrt ergeben sich bei der Bearbeitung von Verdachtsmeldungen, die ursprünglich aus anderen Gründen eingereicht wurden, nicht selten Hinweise auf mögliche Verbindungen zu kriminellen Organisationen. Dabei spielen intermediäre Akteure wie Treuhänder, Anwälte und Vermögensverwalter eine zentrale Rolle. Regionale Schwerpunkte zeigen sich unter anderem im Tessin, im Raum Grono (GR), im Wallis sowie in urbanen Zentren wie Zürich oder Basel; grundsätzlich ist jedoch die gesamte Schweiz betroffen.

Im Jahr 2025 übermittelte die MROS erstmals einen Verdachtsfall von Geldwäscherei im Zusammenhang mit einer möglichen Verletzung von Artikel 60 Absatz 1^{bis} des Bundesgesetzes über den Umweltschutz⁵⁵, einem Deliktsbereich, der typischerweise mit mafiosen Aktivitäten in Verbindung steht. Seit der Gesetzesänderung vom 1. April 2025 kann diese Umweltstraftat als Verbrechen eingestuft werden und somit eine Vortat zur Geldwäscherei darstellen.

Bezüge zu kriminellen Organisationen sind insgesamt schwer zu identifizieren. Viele der Delikte werden im Ausland begangen und die soziale Integration einzelner Beteiligten erschwert die Erkennung und Aufdeckung zusätzlich. In der Analyse muss daher eine Vielzahl von Indikatoren berücksichtigt werden sowie eine enge internationale Zusammenarbeit. In den vergangenen Jahren intensivierte MROS insbesondere die Kooperation mit der Bundesanwaltschaft, der Bundeskriminalpolizei, der italienischen FIU (UIF) sowie mit Euro-pol, um den Informationsaustausch zu stärken und gemeinsame strategische Ansätze weiterzuentwickeln.

⁵³ National Risk assessment 2015 S. 99 – 102 [Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz](#), BAZG foreign trade report 2023 S. 30 – 35 https://www.bazg.admin.ch/dam/de/sd-web/Glgl.22f5YT1m/912.5-02%20jb%202023_1.1_de.pdf.

⁵⁴ <https://www.fedpol.admin.ch/dam/de/sd-web/ux-P5UbPjIB7/strategie-mros.pdf>, <https://www.news.admin.ch/de/nsb?id=103191>, <https://fedpol-ok.ch/de>, <https://www.swissinfo.ch/eng/swiss-politics/fighting-organized-crime-with-a-national-strategy/88241703>.

⁵⁵ USG; SR 814.01.

5 Aus der Praxis der Meldestelle

5.1 Praxisänderung Abbruchmitteilungen – «De-minimis-Praxis»

Mit dem Inkrafttreten von Artikel 9b GwG per 1. Januar 2023 wurde den Finanzintermediären die Möglichkeit eingeräumt, Geschäftsbeziehungen, die Gegenstand einer Verdachtsmeldung sind, nach Ablauf von 40 Arbeitstagen zu beenden, sofern die MROS die übermittelten Informationen nicht zuvor an eine Strafverfolgungsbehörde weitergeleitet hat.

Die praktische Anwendung dieser Bestimmung zeigte, dass ein erheblicher Teil der betroffenen Geschäftsbeziehungen zum Zeitpunkt der Verdachtsmeldung lediglich geringe Vermögenswerte aufwies und nach Ablauf der gesetzlichen Frist regelmässig saldiert wurde. In solchen Konstellationen führte die gesetzlich vorgesehene nachgelagerte Abbruchmitteilung häufig nicht zu einem zusätzlichen Erkenntnisgewinn, sondern verursachte primär administrativen Mehraufwand bei den Finanzintermediären und bei der MROS. Vor diesem Hintergrund führte die MROS im Jahr 2025 eine vereinfachte Praxis ein, die sogenannte «De-minimis-Praxis Abbruchmitteilung». Ziel dieser Anpassung ist es, die Meldeströme in klar abgegrenzten Fällen effizienter zu gestalten und die beteiligten Akteure administrativ zu entlasten. Die neue Praxis wurde im August 2025 im Rahmen eines Newsletters an die Finanzintermediäre kommuniziert.

5.1.1 Kernelemente der neuen Praxis

Die De-minimis-Praxis sieht vor, dass Finanzintermediäre den geplanten Abbruch einer Geschäftsbeziehung bereits **zum Zeitpunkt der Verdachtsmeldung** anzeigen können, sofern die folgenden Voraussetzungen kumulativ erfüllt sind:

- **Geringe Vermögenswerte:** Der Gesamtsaldo der Geschäftsbeziehung beträgt zum Zeitpunkt der Verdachtsmeldung weniger als CHF 15 000.–.
- **Unwiderrufliche Abbruchabsicht:** Der Finanzintermediär legt zum Zeitpunkt der Verdachtsmeldung verbindlich fest, die Geschäftsbeziehung nach Ablauf der 40-tägigen Frist gemäss Artikel 9b GwG zu beenden.
- **Kennzeichnung in der Verdachtsmeldung:** Der Abbruch wird im zweiten Textfeld («Grund für Verdacht») durch die Verwendung des Codes **CANC40** kenntlich gemacht. Der Code bezieht sich auf sämtliche in der Verdachtsmeldung erfassten Geschäftsbeziehungen.

Wird der Abbruch auf diese Weise ex ante mitgeteilt, entfällt die ansonsten erforderliche separate Abbruchmitteilung. Die MROS kennzeichnet entsprechende Meldungen intern. Für die Analyse erforderliche zusätzliche Informationen fordert sie bei Bedarf gestützt auf Artikel 11a GwG ein.

5.1.2 Rechtliche und praktische Grenzen der ex ante Abbruchmitteilung

Rückmeldungen der Finanzintermediäre sowie die ersten Erfahrungen der MROS aus der Umsetzung der neuen Praxis zeigen, dass der tatsächliche Verlauf einer Geschäftsbeziehung zwischen Einreichung der Verdachtsmeldung und vollständiger Saldierung nur eingeschränkt prognostizierbar ist. Dabei sind insbesondere folgende Aspekte zu berücksichtigen:

- **Vermögensbewegungen während der 40-tägigen Frist:** Transaktionen innerhalb dieser Frist können nicht ausgeschlossen werden. Auch geringfügige Zu- oder Abflüsse können für die Analyse relevant sein.
- **Verzögerungen bei der effektiven Saldierung:** Die effektive Kontoauflösung kann sich verzögern, etwa wenn der Kunde keine neue Konto-Verbindung angibt oder operative Abwicklungshindernisse bestehen.
- **Barsaldierungen:** Barsaldierungen bleiben zulässig, sofern weiterhin lediglich geringe Vermögenswerte betroffen sind.

Bis zur tatsächlichen Saldierung bleibt der Finanzintermediär uneingeschränkt verpflichtet, seine Sorgfaltspflichten wahrzunehmen. Dazu gehören insbesondere ein risikobasiertes Monitoring der Geschäftsbeziehung sowie die Einreichung weiterer Verdachtsmeldungen, sofern zusätzliche Verdachtsmomente oder neue relevante Sachverhaltselemente auftreten. In diesen Fällen kann unabhängig von der ursprünglichen Meldung eine erneute Meldepflicht entstehen, wenn zusätzliche Verdachtsmomente oder neue relevante Sachverhaltselemente auftreten.

Die Einführung der De-minimis-Praxis trägt zur gezielten Vereinfachung des Meldeprozesses in klar definierten Konstellationen mit geringen Vermögenswerten bei. Sie verringert redundante Meldungen und senkt den administrativen Aufwand für Finanzintermediäre und der MROS, ohne die Qualität der geldwäschereirelevanten Analyse zu

beeinträchtigen. Gleichzeitig bleibt gewährleistet, dass in Fällen mit erhöhtem Risiko oder potenzieller strafrechtlicher Relevanz weiterhin sämtliche erforderlichen Informationen erhoben und einer sorgfältigen Prüfung unterzogen und weitergeleitet werden können.

5.2 Datenstandard

5.2.1 Datenstandard bei Verdachtsmeldungen

Mit dem kontinuierlichen quantitativen Anstieg der Verdachtsmeldungen gewann das Thema der Datenqualität bei Verdachtsmeldungen auch im Berichtsjahr weiter an Relevanz. Die bestehenden Qualitätsdefizite verschärften sich und führten regelmässig dazu, dass Meldungen oder beigefügte Anhänge zurückgewiesen werden mussten, insbesondere aufgrund unvollständig ausgefüllter Pflichtfelder, fehlerhafter Datenformate oder fehlender strukturierter Angaben. Solche Rückweisungen verursachen bei den meldenden Finanzintermediären zusätzlichen administrativen Aufwand und Verzögerungen. Gleichzeitig beeinträchtigen sie die effiziente Weiterverarbeitung und Analyse der Informationen durch die MROS.

5.2.2 Gesetzliche Neuerung – Artikel 23 Absatz 7 GwG

Mit der jüngsten Revision des Geldwäschereigesetzes wurde diesem Handlungsbedarf Rechnung getragen und eine neue gesetzliche Grundlage geschaffen, welche voraussichtlich im Sommer 2026 in Kraft treten soll. Der neu eingeführte Artikel 23 Absatz 7 GwG legt fest, dass der (Daten-)Verkehr mit der MROS zwingend über das Informationssystem der MROS zu erfolgen hat und ermächtigt fedpol, verbindliche Vorgaben zum Datenstandard der Informationen, die über goAML übermittelt werden, zu erlassen. Damit besteht erstmals eine explizite gesetzliche Grundlage, um formale und strukturelle Anforderungen an den elektronischen Informationsaustausch verbindlich zu regeln. Die bislang als fachliche Empfehlungen ausgestalteten technischen Spezifikationen der MROS, insbesondere jene gemäss dem Handbuch zum Meldesystem goAML sowie dem zugehörigen XML-Schema, erhalten dadurch verbindlichen Charakter. Sie gelten künftig für sämtliche meldepflichtigen Akteure, namentlich Finanzintermediäre sowie Beraterinnen und Berater und Händlerinnen und Händler, aber auch für die Behörden, welche mit

der MROS kommunizieren. Ziel dieser gesetzlichen Regelung ist es, die Einheitlichkeit, Vollständigkeit und formale Qualität der Verdachtsmeldungen nachhaltig sicherzustellen.

5.2.3 Technische Umsetzung – Vorgehen und Perspektive

Gestützt auf Artikel 23 Absatz 7 GwG wird fedpol eine technische Verordnung erarbeiten, welche die Anforderungen an den Datenstandard im Detail konkretisiert. Die Verordnung orientiert sich dabei an den bestehenden Spezifikationen, namentlich am goAML-Handbuch und dem geltenden XML-Schema, welche bereits heute als Referenzrahmen dienen und von einem grossen Teil der meldepflichtigen Akteure angewendet werden.

Die verbindliche Festlegung dieser Standards bezweckt insbesondere die Reduktion formell mangelhafter Meldungen und der damit verbundenen Rückweisungen sowie eine nachhaltige Entlastung der MROS. Gleichzeitig trägt die Standardisierung zur Erhöhung der Rechtssicherheit und zur Gleichbehandlung aller meldepflichtigen Akteure bei. Langfristig sorgt eine klare und verbindliche Regelung zur Datenqualität für eine effizientere automatisierte Verarbeitung, eine verbesserte Nachvollziehbarkeit und Rückverfolgbarkeit der Meldungen und ergänzenden Informationen sowie für verlässlichere Analysen der MROS und effizientere Weiterleitungen an Strafverfolgungsbehörden und ausländische Partnerbehörden. Insgesamt erhöht die Einführung eines einheitlichen und verbindlichen Datenstandards die Wirksamkeit des schweizerischen Dispositivs zur Bekämpfung der Geldwäscherei.

5.2.4 XML Data Quality Report

Ergänzend zur regulatorischen Festlegung des Datenstandards entwickelt die MROS das Instrument XML Data Quality Report. Ziel des XML Data Quality Report Version 1.0 ist es, die Datenqualität der eingehenden Verdachtsmeldungen automatisiert zu messen und systematisch zu überwachen.

Auf dieser Grundlage ist vorgesehen, dass die einzelnen Finanzintermediäre in regelmässigen Abständen standardisierte Berichte zur Datenqualität (DQ-Reports) erhalten. Diese zeigen den Stand und die Entwicklung der Datenqualität der übermittelten

Meldungen auf und ermöglichen eine Einordnung im Verhältnis zu aggregierten Vergleichswerten. Die DQ-Reports dienen ausschliesslich der Qualitätssicherung und sollen die Finanzintermediäre dabei unterstützen, ihre internen Meldeprozesse gezielt weiterzuentwickeln. Für den XML Data Quality Report V1.0 hat die MROS verschiedene Datenqualitäts-Messgrössen definiert. Die Auswahl erfolgte anhand ihres Einflusses auf die nachgelagerten Analyseprozesse sowie ihres Automatisierungspotenzials. Erste Tests mit einer begrenzten Anzahl von Finanzintermediären sind für Q1 2026 vorgesehen. Nach Abschluss der Testphase plant die MROS, ab Mitte 2026 sämtlichen Finanzintermediären die jeweiligen DQ-Reports zur Verfügung zu stellen.

Mit dem XML Data Quality Report wird erstmals ein einheitliches, vergleichbares und kontinuierliches Instrument zur Beurteilung der Datenqualität auf Ebene einzelner Finanzintermediäre eingeführt. Die nachhaltige Sicherstellung einer hohen formellen Qualität der Verdachtsmeldungen ermöglicht der MROS eine effiziente und wirksame Tätigkeit.

6 Internationale Zusammenarbeit in der Bekämpfung der Geldwäscherei

Die Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung setzt eine wirksame internationale Zusammenarbeit voraus. Die MROS arbeitet in multilateralen und bilateralen Kooperationsformaten mit und beteiligt sich sowohl auf operativer als auch auf strategischer Ebene am internationalen Informations- und Erfahrungsaustausch.

Im Oktober 2025 fand in Bern ein Treffen des ECOFEL-Formats statt (siehe hierzu Kapitel 2.7.1). Die stellvertretende Leiterin der MROS nahm ihre Funktion als regionale Vertreterin der Region Europe II im Egmont Committee wahr. Dieser Region gehören unter anderem FIUs aus dem Vereinigten Königreich, Monaco, den Kanalinseln, Israel, Georgien und der Ukraine an.

6.1 Egmont-Gruppe

Die Egmont-Gruppe ist das weltweite Netzwerk der FIUs. Aktuell umfasst sie 182 Mitglieder. Sie dient dem strukturierten Austausch von Informationen, Methoden und Fachwissen.

Vom 27. Januar bis 8. Februar 2025 führte die Egmont-Gruppe ihre 25. Arbeits- und Regionalgruppentreffen durch. Die Sitzungen fanden in virtueller Form statt. Mehr als 800 Vertreterinnen und Vertreter von FIUs, internationalen Partnerorganisationen und Beobachtern nahmen teil. Die Diskussionen befassten sich insbesondere mit Fragen des operativen Informationsaustauschs, mit Effizienzaspekten sowie mit dem Einsatz neuer Technologien.

Die 30. Plenarversammlung der Egmont-Gruppe fand vom 6. bis 11. Juli 2025 in Luxemburg statt. Gastgeberin war die luxemburgische FIU (Cellule de renseignement financier, CRF). Die Plenarversammlung behandelte Fragen der Weiterentwicklung der internationalen Zusammenarbeit zwischen FIUs im Bereich der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung.

Anlässlich dieser Plenarversammlung nahmen auch Vertreterinnen und Vertreter nationaler und internationaler Behörden teil. Verschiedene Wortmeldungen betrafen die Bedeutung der internationalen Kooperation bei der Bekämpfung von Finanzkriminalität.⁵⁶

Die MROS beteiligte sich im Berichtsjahr an den Arbeiten der Egmont-Gruppe. Vom 14. bis 15. Ok-

6.2 Financial Action Task Force (FATF)

Die FATF⁵⁷ setzte ihre Arbeiten zur Weiterentwicklung der internationalen Standards zur Bekämpfung von Geldwäscherei, Terrorismus- und Proliferationsfinanzierung im Jahr 2025 fort.

Anfang Januar 2025 fand in Wien das jährliche Joint Expert Meeting (JEM) statt. Die Arbeiten gliederten sich in die Themenbereiche Vermögensabschöpfung (Asset Recovery) und Terrorismusfinanzierung.

Vom 19. bis 21. Februar 2025 führte die FATF in Paris ihre erste Plenarsitzung des Jahres durch. Delegationen aus dem globalen Netzwerk der FATF sowie Beobachter internationaler Organisationen nahmen an den fachlichen Beratungen teil.⁵⁸ Behandelt wurden unter anderem Anpassungen der FATF-Standards zur Stärkung des risikobasierten Ansatzes unter Berücksichtigung der finanziellen Inklusion sowie ein Bericht zu Finanzströmen im Zusammenhang mit der sexuellen Ausbeutung von Kindern im Internet.⁵⁹

Am 12. und 13. Juni 2025 fand eine gemeinsame Plenarsitzung mit Moneyval statt. Moneyval ist das Evaluationsgremium des Europarates für jene Mitgliedstaaten, die nicht der FATF angehören. In diesem Rahmen beschlossen die Teilnehmenden unter anderem Anpassungen der Empfehlung 16 zur Erhöhung der Transparenz bei grenzüberschreitenden Zahlungen. Für grenzüberschreitende Transaktionen in der Höhe von mehr als USD/EUR 1000 sind künftig eindeutige Angaben zu Auftraggebenden und Begünstigten erforderlich. Die

⁵⁶ [Luxembourg's FIU \(CRF\) hosts the 30th anniversary of the Egmont Group at this year's Plenary – Egmont Group.](#)

⁵⁷ Zum Aufbau und den Aufgaben der Organisation vgl. [Jahresbericht MROS 2023](#), Kap. 7.2.

⁵⁸ [Outcomes FATF Plenary, 19 – 21 February 2025.](#)

⁵⁹ [Detecting, Disrupting and Investigating Online Child Sexual Exploitation.](#)

Finanzintermediäre haben diese Anforderungen bis spätestens 2030 umzusetzen.⁶⁰

Die dritte Plenarsitzung des Jahres fand vom 22. bis 24. Oktober 2025 in Paris statt. Dabei verabschiedete die FATF unter anderem Länderberichte zu Belgien und Malaysia.

Im Berichtsjahr passte die FATF zudem die Zusammensetzung der sogenannten «grauen Liste» an. Diese umfasst Jurisdiktionen mit strategischen Defiziten in ihren Systemen zur Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung, die einer verstärkten Überwachung unterliegen. Neu aufgenommen wurden unter anderem Laos, Nepal, Bolivien und die Britischen Jungferninseln. Von der Liste gestrichen wurden unter anderem die Philippinen, Kroatien, Mali, Tansania, Burkina Faso, Mosambik, Nigeria und Südafrika.

Im Februar 2024 veröffentlichte die FATF eine risikobasierte Leitlinie zur Umsetzung der Empfehlung 25 betreffend Transparenz bei wirtschaftlich berechtigten Personen von Rechtskonstrukten.⁶¹ Vor diesem Hintergrund verabschiedete die Schweiz am 26. September 2025 das TJPG. Das vorgesehene nicht öffentliche Register soll den zuständigen Behörden den Zugang zu Informationen über wirtschaftlich berechnete Personen ermöglichen. Die Vernehmlassung zur Ausführungsverordnung wurde im Oktober 2025 eröffnet. Das Inkrafttreten ist für die zweite Hälfte 2026 vorgesehen.⁶²

Schliesslich ernannte die FATF ihren neuen Vizepräsidenten für die Amtsperiode vom 1. Juli 2025 bis zum 30. Juni 2027.⁶³

6.3 Taskforces

Die MROS beteiligte sich im Berichtsjahr an mehreren operativen und strategischen Taskforces. Dazu zählen insbesondere die Russia-Related Illicit Fi-

nance and Sanctions FIU Working Group (RRIFS)⁶⁴ sowie die Counter Terrorist Financing Task Force (CTFT).⁶⁵ Beide Formate dienen dem Austausch zu aktuellen Risiken, Fallkonstellationen und methodischen Fragen. Im Jahr 2025 fanden mehrere Sitzungen statt, an denen die MROS mitwirkte.

6.4 Bilaterale Treffen

Die MROS pflegte im Berichtsjahr den direkten Austausch mit ausländischen Partner-FIUs. Diese Kontakte dienen dem Verständnis der jeweiligen rechtlichen Rahmenbedingungen und Informationszugänge der Partnerbehörden. Sie unterstützen eine effiziente Fallbearbeitung und tragen zu einem zielgerichteten Ressourceneinsatz bei. Zudem ermöglichen sie einen strategischen Austausch zu Entwicklungen in den Bereichen organisierte Kriminalität und Terrorismusfinanzierung sowie zu technischen Fragen des Datenaustauschs.

Im Jahr 2025 führte die MROS bilaterale Gespräche unter anderem mit den FIUs von Frankreich, den Vereinigten Staaten, Nigeria, Italien, den Vereinigten Arabischen Emiraten, Katar, Bahrain, Österreich, Monaco, Liechtenstein und Deutschland.

Die deutsche FIU organisierte im Dezember 2025 ein deutschsprachiges FIU-Treffen. Thematisiert wurden insbesondere der Umgang mit steigenden Datenvolumen im Verhältnis zu verfügbaren Ressourcen sowie die Vorbereitung auf anstehende FATF-Länderevaluationen.

Im Berichtsjahr schloss die MROS zudem Memoranda of Understanding mit den FIUs von Frankreich, Kasachstan, China und Island ab. Diese Vereinbarungen regeln den Rahmen für den Informationsaustausch und die operative Zusammenarbeit.

⁶⁰ [Outcomes Joint FATF-MONEYVAL Plenary, 12 – 13 June 2025.](#)

⁶¹ [FATF, Guidance on Beneficial Ownership and Transparency of Legal Arrangements.](#)

⁶² [Bundesrat eröffnet Vernehmlassung zu Verordnungen über die Transparenz juristischer Personen und die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung.](#)

⁶³ [Outcomes FATF Plenary, 19 – 21 February 2025.](#)

⁶⁴ [Russia-Related Illicit Finance and Sanctions FIU Working Group \(RRIFS Task Force\).](#)

⁶⁵ [Counter Terrorist Financing Taskforce \(CTFT\).](#) Hinweis: Der Name der Taskforce wurde mittlerweile von CTFTI zu CTFT geändert und der Fokus liegt nun auf der allgemeinen Bekämpfung der Terrorismusfinanzierung.

7 Organisation der MROS

Die MROS ist organisatorisch dem Direktionsbereich Kriminalprävention & Recht von fedpol angegliedert. In ihrer operativen Kerntätigkeit agiert die MROS vollständig unabhängig und setzt damit die internationalen Anforderungen um.

Im Jahr 2025 war die MROS in sechs Fachbereiche gegliedert. Sie beschäftigte durchschnittlich 66 Mitarbeitende, entsprechend 57 Vollzeitäquivalenten (VZÄ).

Die Aufbauorganisation ergibt sich aus dem Organigramm und bildet die funktionale Gliederung der Aufgaben der MROS ab.

Planung und Policy (PuP)

Der Bereich PuP nimmt die Querschnittsaufgaben der MROS wahr. Er bearbeitet sämtliche juristischen, politischen und strategischen Dossiers bis auf Stufe Bundesrat, insbesondere Gesetzgebungsprojekte, strategische Dokumente und parlamentarische Vorstösse. Zudem verantwortet der Bereich die Koordination und Umsetzung von Projekten und Publikationen der MROS. PuP stellt die Einheitlichkeit der fachlichen Auslegung sicher, unterstützt die operativen Bereiche in rechtlichen und konzeptionellen Fragen und ist für das Risikomanagement zuständig. Die administrativen Belange der MROS sowie der Austausch mit anderen Behörden sind ebenfalls in diesem Bereich angesiedelt.

Primäranalyse (PA)

Der Bereich PA ist für die Entgegennahme, formelle Prüfung und inhaltliche Erfassung sämtlicher eingehender Verdachtsmeldungen verantwortlich. Dazu gehören insbesondere die technische und formale Aufbereitung der Meldungen sowie erforderliche manuelle Korrekturen bei unzureichender Datenqualität. Darüber hinaus übernimmt sie die Triage, übergibt die Fälle anhand einer Gesamtbewertung an einen der nachgelagerten operativen Bereiche oder bearbeitet und leitet Meldungen direkt an Strafverfolgungsbehörden weiter. Ebenfalls in ihre Zuständigkeit fällt die nationale Amtshilfe nach Artikel 29 GwG.

Operative Analyse Kantone (OAK)

Der Bereich OAK analysiert eingehende Verdachtsmeldungen, welche überwiegend in die Zuständigkeit der kantonalen Strafverfolgungsbehörden fallen und vom Bereich PA zugewiesen wurden. Bei Vorliegen eines begründeten Verdachts werden die aggregierten und analysierten Informationen an die jeweils zuständige Strafverfolgungsbehörde übermittelt. Informationen können im Zuge eines Informationsaustausches auch mit anderen nationalen Behörden sowie FIUs anderer Länder geteilt werden. Die Fälle betreffen u. a. die strafbaren Handlungen gegen das Vermögen (hauptsächlich Betrug, Veruntreuung und ungetreue Geschäftsbesorgung), Menschenhandel und Urkundenfälschung.

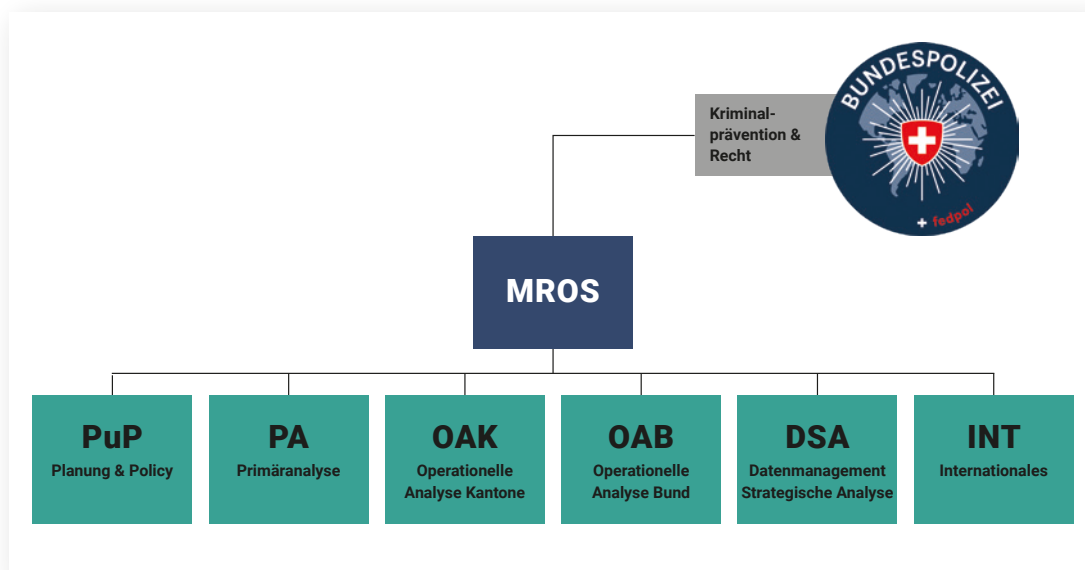


Abbildung 12: Organigramm MROS

Operative Analyse Bund (OAB)

Der Bereich OAB analysiert eingehende Verdachtsmeldungen, welche a priori in die Zuständigkeit der BA fallen und vom Bereich PA zugewiesen wurden. Bei begründetem Verdacht werden die aggregierten Informationen an die zuständige Strafverfolgungsbehörde übermittelt (in der Regel BA bzw. gegebenenfalls auch kantonale Strafverfolgungsbehörden). Informationen können im Zuge eines Informationsaustausches auch mit anderen nationalen Behörden sowie FIUs anderer Länder geteilt werden. Die Fälle betreffen u. a. internationale Geldwäscherei (hauptsächlich Bestechung), organisierte Kriminalität, Terrorismus, Börsendelikte, Rechts- und Linksextremismus sowie Sanktionsumgehung (schwere Verstösse gegen das Embargogesetz).

Datenmanagement und strategische Analyse (DSA)

Der Bereich DSA ist für den sicheren Betrieb des Informationssystems der MROS (goAML) sowie für dessen fachliche und technische Weiterentwicklung verantwortlich. Er stellt den technischen Support für meldepflichtige Akteure sicher, insbesondere im Zusammenhang mit der Anbindung und dem Betrieb von Schnittstellen. DSA ist zudem für die Entwicklung der technischen Möglichkeiten der Datenverarbeitung im Zusammenhang mit Verdachtsmeldungen zuständig. Der Bereich führt die strategischen Analysen der MROS aus und wertet unterschiedlichste Daten im Zusammenhang mit der Bekämpfung von Geldwäscherei, deren Vortaten und Terrorismusfinanzierung aus, um Risiken, Tendenzen und Methoden der Geldwäscherei zu identifizieren.

Internationales (INT)

Der Bereich INT verantwortet den gesamten (Informations-)Austausch mit ausländischen FIUs. Er koordiniert zudem die Mitgliedschaft der MROS in internationalen Gremien und ihre Teilnahme an multilateralen und bilateralen Kooperationsformaten (u. a. Egmont Group, GAFI / FATF, United Nations Convention against Corruption (UNCAC) und EFIPPP).

