Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2024

Mai 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2024

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

Auch für das Jahr 2024 gibt es praktisch in sämtlichen Reporting-Kategorien wiederum Rekordwerte zu vermelden. Insgesamt registrierte die Meldestelle für Geldwäscherei (MROS[1]) in ihrem Informationssystem goAML[2] 27 901 Eingänge. Im Vergleich zum Vorjahr entspricht dies einer Zunahme von knapp 30%. Seit der Einführung von goAML im Jahr 2020 hat sich das eingehende Datenvolumen mehr als verdreifacht. Im Durchschnitt erhält die MROS pro Werktag 107 Reports: Verdachtsmeldungen (STR[3]s/SAR[4]s), Antworten der Finanzintermediäre auf Anfragen der MROS[5], Abbruchsmitteilungen[6], internationale Anfragen von Financial Intelligence Units (FIUs), Spontaninformationen, Anfragen und Antworten von nationalen und internationalen Behörden sowie Urteilszustellungen der Strafbehörden[7].

Im Jahr 2024 sind bei der MROS insgesamt 15 141 Verdachtsmeldungen eingegangen. Dies entspricht einer Zunahme von 27,5% im Vergleich zum Vorjahr (2023: 11 876). Im Durchschnitt werden somit 59 Meldungen pro Werktag verzeichnet. Der Anteil der Verdachtsmeldungen an den eingehenden Reportings beträgt rund 55%. Dieser Wert hat sich in den letzten Jahren stetig verringert – noch vor 10 Jahren lag der Anteil bei den Verdachtsmeldungen am Gesamtvolumen bei über 90%. Diese Entwicklung ist darauf zurückzuführen, dass die Amtshilfetätigkeit zwischen der MROS und den nationalen Behörden aber auch mit den internationalen Partnerstellen stark zugenommen hat. Sie zeigt deutlich, dass sich die Behörden heute häufiger vernetzen und Abklärungen bei externen Stellen durchführen. Dies gilt namentlich auch für die MROS. Financial Intelligence lebt von einem aktiven Informationsaustausch und der Interaktion mit den verschiedenen Stakeholdern. Um hohe Datenvolumen effizient verarbeiten zu können, bedarf es Reportings, die strukturiert sind und formell aber auch inhaltlich eine gewisse Mindestqualität aufweisen. Die MROS stellt nach wie vor einen Unterschied in der Qualität bei den Verdachtsmeldungen fest. Grund hierfür dürfte der Kostendruck sein – zudem besteht aber offenbar auch ein Spannungsverhältnis zwischen der «Unverzüglichkeit» und der «Abklärungstiefe» einer Verdachtsmeldung (vgl. Kap. 5.1).

Im Jahr 2024 hat die MROS insgesamt 1043 Anzeigen an die Strafverfolgungsbehörden übermittelt. Gegenüber dem Vorjahr konnten die Anzeigen somit um mehr als 20% gesteigert werden. Die MROS stellt den Strafverfolgungsbehörden jeweils einen Analysebericht mit den relevanten Informationen zur Verfügung. Diese können aus mehreren Verdachtsmeldungen hervorgehen, die nicht zwingend im selben Jahr bei der MROS eingegangen sind und Informationen von verschiedenen in- und ausländischen Behörden enthalten. 2024 übermittelte die MROS im Schnitt 1,9 Verdachtsmeldungen pro Anzeige. Die durchschnittliche Anzahl der Verdachtsmeldungen, die pro Anzeige an die Strafverfolgungsbehörden übermittelt wurden, hat über die letzten Jahre zugenommen (2021: 1,3, 2022: 1,4, 2023: 1,8). Rund jede fünfte Übermittlung an die Strafverfolgungsbehörden beinhaltete zudem Informationen basierend auf einer oder mehreren Anfragen der MROS nach Artikel 11*a* GwG[8] bei meldenden Finanzintermediären oder Drittintermediären. Die MROS hat zudem im Jahr 2024 verstärkt Gebrauch vom Instrument der Spontaninformation (Art. 29 GwG) gemacht. Insgesamt hat sie 358 Spontaninformationen an inländische Behörden getätigt. Dies entspricht einer Zunahme von 79% gegenüber dem Vorjahr. Die MROS setzt ihre Informationen gezielt ab und bindet die empfangenden Behörden frühzeitig in die Übermittlung ein.

Die Anzahl der Anzeigen an die Strafverfolgungsbehörden sagt nur bedingt etwas über die Effizienz und die Effektivität der Analysetätigkeit aus. Es ist einerseits der Gesamtoutput zu berücksichtigen; Analysen, die zu Anzeigen und Spontan-

[1] Money Laundering Reporting Office Switzerland.
[2] «government office Anti Money Laundering».
[3] Suspicious Transaction Report.
[4] Suspicious Activity Report.
[5] Anfragen der MROS gestützt auf Art. 11*a* GwG.
[6] Gestützt auf Art. 9*b* GwG.
[7] Gestützt auf Art. 29*a* GwG.
[8] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG), SR 955.0.

informationen beitragen. Weiter ist der Durchlauf massgeblich; wie viele Informationen werden tatsächlich im Rahmen einer Analyse verarbeitet. Bei beiden Kennzahlen hat sich die MROS im letzten Jahr gesteigert.

Die MROS hat für die Periode 2024 – 2027 ihre strategischen Ziele und ihr Profil hinsichtlich ihrer gesetzlich definierten Kernaufgaben neu formuliert. Dabei hat sie die drei Bereiche «Intelligence», «Kooperation» und «Prävention» geschärft (vgl. Kap. 2.1). Im Zentrum ihrer Überlegungen standen ebenfalls die zukünftigen Herausforderungen, die sich für eine FIU stellen und welche Fähigkeiten und Instrumente die MROS zukünftig benötigt, um diese zu meistern. Die Herausforderungen werden mittels einer Studie ermittelt, die voraussichtlich im 2025 abgeschlossen sein wird (vgl. Kap. 2.4).

Am 7. November 2024 nahm die Swiss Financial Intelligence Public Private Partnership («Swiss FIPPP»), bestehend aus 12 Finanzinstituten und der MROS, ihre Tätigkeit offiziell auf. Damit verfügt der Schweizer Finanzplatz über eine Public Private Partnership und schliesst zu den anderen internationalen Finanzzentren auf (vgl. Kap. 2.3). Ende Oktober 2024 führte die MROS eine zweite Auflage des Crypto-Symposiums durch. Der Anlass richtete sich an die im Bereich Krypto- und Virtual-Assets tätige Finanzindustrie. Die Rückmeldungen waren sehr positiv. Gerade in diesem noch jungen Finanzsegment ist der Austausch zwischen Behörden und Industrie äusserst wichtig. Entsprechend wird die MROS 2025 den Anlass in gleichem Rahmen durchführen (vgl. Kap. 2.5.3). Im vorliegenden Jahresbericht wird auf die Rubrik «Typologien» verzichtet und auf einen Typologienbericht auf der Homepage der MROS verwiesen (vgl. Kap. 2.5.2). Dies ermöglicht der MROS, die Finanzbranche auch unterjährig mit aktuellen Fallstudien zu bedienen.

2 Wichtige strategische Entwicklungen

2.1 Ausrichtung und Zielsetzungen der MROS für die Periode 2024 – 2027

Die MROS ist die zentrale Meldestelle für Verdachtsfälle im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung in der Schweiz und nimmt die Aufgaben einer Financial Intelligence Unit (FIU) wahr. Das in Gesetz und Verordnung umschriebene Mandat der MROS umfasst dabei die folgenden drei Kernaufgaben:

- **Intelligence:** Die Meldestelle empfängt Verdachtsmeldungen, welche gestützt auf das Geldwäschereigesetz und das Strafgesetzbuch[9] von Finanzintermediären sowie Händlerinnen und Händlern erstattet werden. Sie führt eigene Analysen durch und ergänzt die erhaltenen Verdachtsmeldungen mit Informationen. Sie entscheidet daraufhin im Einzelfall, ob eine Anzeige an eine Strafverfolgungsbehörde übermittelt wird oder nicht.
- **Kooperation:** Die Meldestelle tauscht sich mit anderen nationalen Behörden sowie mit ausländischen FIUs auf dem Weg der Amtshilfe aus, in operativen und strategischen Belangen.
- **Prävention:** Die Meldestelle trägt zur Bewertung der nationalen Risiken von Geldwäscherei und Terrorismusfinanzierung bei. Sie erstellt strategische Analysen und teilt die gewonnenen Erkenntnisse mit den Behörden, der Finanzindustrie sowie der Öffentlichkeit.

Diese drei Kernaufgaben sind dabei nicht isoliert zu betrachten, sondern formen eine Einheit. Fundament bildet die Intelligence: Darauf baut die Kooperation und die Prävention auf.

Für die Periode 2024 – 2027 hat die Meldestelle ihre strategischen Ziele, welche sich aus ihrem gesetzlichen Auftrag ableiten, neu formuliert.[10] Diese zeigen auf, wie die Meldestelle ihr gesetzliches Mandat erfüllt, welche Schwerpunkte sie setzt und wie sie ihren Handlungsspielraum nutzt. Die periodisch neu festgelegten Ziele sind eine Antwort auf die Entwicklungen in der Geldwäscherei- und Kriminalitätsbekämpfung und den damit verbundenen Herausforderungen. Sie bilden eine Verbindung zwischen dem gesetzlichen Auftrag und der konkreten Tätigkeit der MROS.

Die neue Strategie der MROS definiert sechs Ziele und dreizehn Massnahmen. Sie setzt klare Prioritäten auf die Schwerstkriminalität und bietet mit ihren Analysen einen Mehrwert in der Kriminalitätsbekämpfung für ihre direkten Partner – nationale Behörden, ausländische FIUs sowie die Finanzindustrie. Die jährlich stetig steigende Anzahl der unterschiedlichen Reportings und die knappen Ressourcen zwingen die MROS dazu, risikobasiert zu agieren.[11] Nebst einem konsequenten Fokus auf gewisse Deliktsfelder, setzt die MROS in ihrer Strategie auf die Straffung der Melde- und Verarbeitungsprozesse. Ein weiterer Schwerpunkt stellt die Weiterentwicklung der IT-Infrastruktur dar. Zeitgemässe und moderne Analysetools sind der Schlüssel, um Massendaten effizient zu bearbeiten und aussagekräftige Analysen zu erstellen. Wesentlich ist auch eine aktive und gezielte Zusammenarbeit mit verschiedenen Stakeholdern: mit dem Privat- und Finanzsektor, den nationalen Behörden und den internationalen Partnerstellen. In einem globalen Umfeld lässt sich Finanzkriminalität nur gemeinsam bekämpfen. Es ist zentral, die Parteien an einen Tisch zu bringen und Problemstellungen gemeinsam anzugehen.

2.2 Nationale Risikoanalyse (NRA) – Sektorieller Bericht zu Proliferationsfinanzierung

Die Beurteilung der Risiken, die durch Geldwäscherei und Terrorismusfinanzierung entstehen, sind ein wichtiger Bestandteil der Kriminalitätsbekämpfungsstrategie der Schweiz. Entsprechend hat die Schweiz bereits zwei umfassende nationale

[9] Schweizerisches Strafgesetzbuch, SR 311.0.

[10] Vgl. Strategie MROS 2024 – 2027, abrufbar unter: https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/strategie-mros.pdf.download.pdf/strategie-mros-d.pdf.

[11] Vgl. hierzu die Ausführungen zum risikobasierten Ansatz im Jahresbericht MROS 2023, Kap. 2.2.

Risikoanalysen (NRA) publiziert (2015[12] und 2021[13]), in denen die Risken bewertet wurden. Auftraggeberin und verantwortlich für die Erstellung der NRAs ist die Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). Die MROS ist Teil dieser Koordinationsgruppe; als Leiterin der Untergruppe «Risikoanalyse» ist sie verantwortlich für die Erstellung der Risikoberichte. Die KGGT verfasst in regelmässigen Abständen NRAs zu risikobehafteten Themengebieten und aktualisiert diese laufend.

Neben der übergreifenden Risikobeurteilung veröffentlicht die KGGT regelmässig sektorielle Risikoanalysen. Am 17. September 2024 verabschiedete sie den sektoriellen Risikobericht «National Risk Assessment: Proliferationsfinanzierung», den die MROS in Zusammenarbeit mit dem Staatssekretariat für Wirtschaft (SECO) erstellte.[14]

Die Verbreitung von Massenvernichtungswaffen und ihren Trägersystemen stellen eine Gefahr für den Frieden und die internationale Sicherheit dar. Der Verhinderung der Finanzierung für die Verbreitung von Massenvernichtungswaffen (Proliferationsfinanzierung) liegt ein komplexer internationaler und nationaler Rechtsrahmen zugrunde. Der Bericht skizziert die globale Risikolandschaft und die spezifischen Proliferationsfinanzierungsrisiken, mit einem Fokus auf Iran und Nordkorea.

Für die Schweiz kommt die Risikoanalyse insbesondere zu folgenden Erkenntnissen:

- Im Rohstoffhandel, im Handel mit Kryptowährungen und im Korrespondenzbankgeschäft werden die Risiken der Proliferationsfinanzierung am grössten eingeschätzt. Zudem besteht ein übergreifendes Risiko aufgrund von Umgehungsgeschäften durch Tarnfirmen.
- Der Iran stellt handelsbezogene Risiken dar, da das Land im Gegensatz zu Nordkorea nicht von der Wertschöpfungskette ausgeschlossen ist. Nordkorea hingegen stellt ein höheres Risiko im Bereich der Cyberkriminalität und der damit verbundenen Nutzung von Kryptowährungen dar.

Der Bericht empfiehlt, das Abwehrdispositiv im Bereich der Proliferationsfinanzierung zu stärken, indem das Mandat der KGGT um die Proliferationsfinanzierung erweitert und eine interdepartementale Arbeitsgruppe zu diesem Thema gebildet wird. Darüber hinaus muss die Datengrundlage verbessert und der Privatsektor besser sensibilisiert werden.

2.3 Public-Private-Partnership (PPP) – Swiss FIPPP

Der Informationsaustausch zwischen Behörden und dem Privatsektor verbessert die Wirksamkeit in der Geldwäschereibekämpfung. Deswegen sollten diese gezielt zusammenarbeiten und Informationen über Bedrohungen, Risiken, Methoden und Tendenzen im Bereich der Geldwäscherei und Terrorismusfinanzierung austauschen können. In den letzten zehn Jahren wurden auf internationaler Ebene verschiedene öffentlich-private Partnerschaften zum Austausch von Finanzinformationen gebildet (sog. Public Private Partnerships).

Abbildung 1: Logo Swiss FIPPP.

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

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

[14] Medienmitteilung Bundesrat vom 9. Dezember 2024, «Bericht zum Risiko der Proliferationsfinanzierung».

Diese Entwicklung nahm auch die Schweiz zum Anlass, eine eigene PPP im Bereich der Geldwäscherei und Terrorismusfinanzierung zu lancieren. Am 7. November 2024 nahm die Swiss Financial Intelligence Public Private Partnership («Swiss FIPPP») anlässlich einer konstituierenden Plenarsitzung ihre Tätigkeit auf.[15] Dem offiziellen Start der Swiss FIPPP gingen rund zwei Jahre Vorbereitungsarbeiten voraus. Analysiert wurde, in welchem Rahmen eine öffentlich-private Zusammenarbeit in der Schweiz möglich ist.[16] Im Zentrum der Partnerschaft zwischen der MROS und Schweizer Finanzmarktteilnehmern steht der Austausch von Informationen im strategischen Bereich, um Risiken und Bedrohungen erkennen und das Abwehrdispositiv gemeinsam und nachhaltig stärken zu können. Eine taktisch orientierte Zusammenarbeit, bei der Informationen zu konkreten Fällen und Personen ausgetauscht werden, ist derzeit nicht vorgesehen und bräuchte gesetzliche Anpassungen. Die Swiss FIPPP besteht zwischen der MROS und zunächst zwölf initiierenden Finanzinstituten: Bank Julius Bär & Co AG, Bank Vontobel AG, Banque Lombard Odier & Cie SA, Bitcoin Suisse AG, Deutsche Bank (Schweiz) AG, HSBC Private Bank (Suisse) SA, Raiffeisen Schweiz Genossenschaft, Societe Generale Corporate & Investment Banking, UBS AG, Valiant Bank AG, Zürcher Kantonalbank und Zürich Versicherungs-Gesellschaft AG. Es ist nicht ausgeschlossen, dass sich der Kreis der Mitglieder verändern kann.

Eine Plenarsitzung sämtlicher Mitglieder ist mindestens zwei Mal jährlich vorgesehen. Zudem treffen sich themenspezifische Arbeitsgruppen regelmässig. Die Aktivitäten der Swiss FIPPP werden von einem Vorstand koordiniert, deren Mitglieder von der Plenarversammlung gewählt werden. Organisation und Kommunikation stellt die MROS sicher. Swiss FIPPP wird über ihre Tätigkeiten und die gewonnen Erkenntnisse sowohl in einem Jahresbericht als auch ad-hoc gezielt und adressatengerecht informieren.

2.4 Financial Intelligence Unit (FIU) 2.0

In ihrem Gründungsjahr 1998 beschäftigte die MROS vier Mitarbeitende und erhielt 173 Verdachtsmeldungen. 26 Jahre später hat sich der Personalbestand der MROS auf rund 55 Mitarbeitende erhöht und die Verdachtsmeldungen haben sich um ein x-Faches auf 15 000 multipliziert. Im Jahresbericht 2023 erläuterte die MROS die regulatorischen und operativen Gründe für diesen markanten Anstieg des Meldevolumens.[17] Doch was bedeuten diese Entwicklungen für die FIUs aus organisatorischer Sicht? Was benötigen die FIUs, um ihren gesetzlichen Auftrag und die damit verbundenen Aufgaben auch in Zukunft erbringen zu können?

Geldwäscherei ist der zentrale Motor der organisierten Kriminalität und hat in den letzten Jahren deutlich an Komplexität zugelegt. Durch internationale Netzwerke, adaptierte Geldwäschereitechniken sowie den Einsatz neuer Technologien (z. B. Virtual Assets) wird die Bekämpfung der Geldwäscherei und Terrorismusfinanzierung zusehends schwieriger und aufwändiger. Während sich die Tätigkeit der MROS in der Vergangenheit vorwiegend auf das Entgegennehmen und das Weiterleiten der Verdachtsmeldungen beschränkte, hat sich in den letzten Jahren der Fokus klar in Richtung «Intelligence» verschoben. Die Vernetzung der Informationen, die Schaffung von Mehrwerten für die nachgelagerten Strafverfolgungsbehörden durch konzise Analysen und die Interaktion mit den nationalen Behörden und den internationalen Partnerstellen sowie der Finanzindustrie stehen heute im Vordergrund. Diese Tätigkeiten sind notwendig, um Geldwäscherei und Terrorismusfinanzierung effektiv zu bekämpfen. Dies bedingt aber zwingend die Weiterentwicklung der Meldestellen in zentralen Bereichen der IT-Infrastruktur und des Personalwesens, um mit den weltpolitischen Entwicklungen mitzuhalten und die wachsenden Aufgaben und Anforderungen erfüllen zu können.

IT-Infrastruktur

FIUs benötigen für ihre Arbeit Softwarelösungen, die innerhalb der rechtlichen Vorgaben (insbesondere datenschutzrechtliche Bestimmungen)

[15] Swiss Financial Intelligence Public Private Partnership (Swiss FIPPP)

[16] Bericht der Meldestelle: Public Private Partnership (PPP) zum Informationsaustausch für die Bekämpfung von Terrorismusfinanzierung und Geldwäscherei, März 2023.

[17] Vgl. Jahresbericht MROS 2023, Kap. 2.1.

den Anforderungen an eine FIU und den globalen Entwicklungen gerecht werden. Die Fähigkeit, grosse Datenmengen aus verschiedenen Quellen, einschliesslich Open Source Intelligence (OSINT), zu sammeln und zu analysieren, wird immer wichtiger. FIUs müssen in der Lage sein, Informationen aus Finanztransaktionen und Datenbanken sowie OSINT-Quellen zu interpretieren. Künstliche Intelligenz und maschinelles Lernen spielen hierbei eine entscheidende Rolle, um verdächtige Aktivitäten frühzeitig zu erkennen und zu identifizieren. Neue Technologien bieten FIUs die Möglichkeit, ihre Effektivität zu steigern und ihr Verständnis für die Bedrohungen aus der Geldwäscherei und der Terrorismusfinanzierung zu vertiefen.

Personalplanung

Die Komplexität der zu analysierenden Sachverhalte, die rechtlichen Fragestellungen sowie der Einsatz von spezifischen Tools verlangen nach einer strategischen Personalplanung der FIUs. Die Rekrutierung von Spezialistinnen und Spezialisten, wie auch die Bindung von qualifizierten Mitarbeitenden spielen eine zentrale Rolle. FIUs müssen attraktive Arbeitsbedingungen bieten und über die notwendigen liquiden Mittel verfügen, um Talente langfristig gewinnen und binden zu können. FIUs benötigen Handlungsspielraum, um Ressourcen gezielt einzuplanen und einzusetzen.

Der rasante technische Fortschritt, der für Geldwäscherei und Terrorismusfinanzierung immer mehr und immer zugänglichere Möglichkeiten bietet, stellt die FIUs weltweit (nicht nur in der Schweiz) vor gewaltige Herausforderungen. Die MROS befindet sich als Teil der Bundesverwaltung in einem Spannungsfeld zwischen einem kontinuierlich ansteigenden Melde- und Datenvolumen, begrenzten Ressourcen und Budgetvorgaben sowie bestehendem Rechtsrahmen. Trotz allem ist sie darauf angewiesen, für die Bekämpfung der Schwerstkriminalität mit den notwendigen und sachgerechten Instrumenten ausgestattet zu sein. Die vorgenannten Limitationen dürfen nicht gänzlich im Widerspruch zur Notwendigkeit dieser Instrumente stehen. Eine Abwägung, welche auf die Effektivität einer FIU abzielt, ist erforderlich.

Die MROS wird vor diesem Hintergrund im Jahr 2025 eine Studie zum Thema «FIU 2.0» vorlegen, welche die erwähnten Herausforderungen behandelt und entsprechend Lösungsvorschläge anbietet. Teil davon ist auch eine Benchmarkanalyse, die Aufschluss über ihr Standing im internationalen Vergleich gibt.

2.5 Projekte und Veranstaltungen MROS

Im 2024 lancierte die MROS nachfolgende Projekte und Veranstaltungen. Diese haben das Ziel, nützliche Instrumente für Behörden und den Privatsektor zur Verfügung zu stellen und diese entsprechend zu sensibilisieren. Allesamt liefern wichtige Trends und Indikatoren, um die Geldwäscherei und Terrorismusfinanzierung flächendeckender zu bekämpfen.

2.5.1 Financial Intelligence against Human Trafficking (FIAHT)

Menschenhandel ist einer der lukrativsten Zweige der organisierten Kriminalität. Es ist ein im Verborgenen stattfindendes, transnationales Verbrechen. Gemäss Schätzungen der International Labour Organisation erzielt der Menschenhandel weltweit jährlich Gewinne in der Höhe von 236 Milliarden USD. Dessen Zweck ist ausnahmslos der finanzielle Gewinn, der durch die Ausbeutung der Opfer erreicht wird. Die vertiefte Analyse von Zahlungsströmen und Kontobewegungen, die sogenannte «Follow-The-Money»-Strategie, wie sie die MROS verfolgt, leistet einen wesentlichen Beitrag zur Aufdeckung illegaler Aktivitäten rund um den Menschenhandel und zur Identifikation dessen Opfer.

FIAHT Financial Intelligence against Human Trafficking

Abbildung 2: Logo Projekt «Financial Intelligence Against Human Trafficking» (FIAHT)

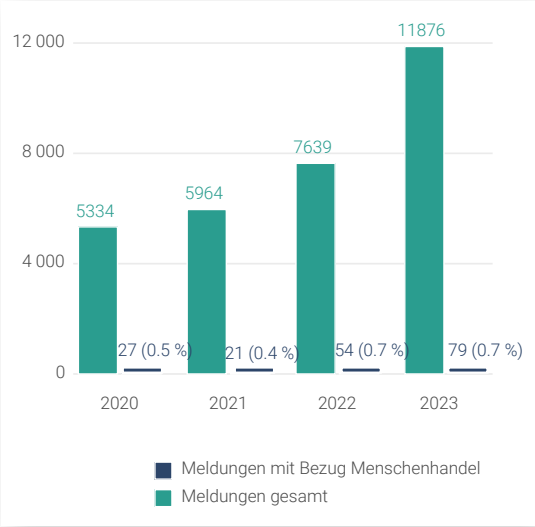


Abbildung 3: Meldungen an die MROS mit Verdacht auf Menschenhandel im Vergleich zum Total der eingegangenen Verdachtsmeldungen; 2020 – 2023.

Hintergrund

Die Schweizerische Gesetzgebung qualifiziert Menschenhandel als Vortat zu Geldwäscherei. Die Finanzintermediäre sind deshalb verpflichtet, der MROS bei Verdacht auf Menschenhandel und verwandter Straftaten, Meldung zu erstatten. In der Schweiz, wie auch in vielen anderen europäischen Ländern, bewegt sich die Anzahl der Verdachtsmeldungen mit Hinweisen auf Menschenhandel auf einem ausserordentlich tiefen Niveau; es besteht eine grosse Diskrepanz zwischen dem Ausmass dieses Verbrechens und den durch die Finanzintermediäre erstatteten Verdachtsmeldungen.

Projekt FIAHT

Die MROS lancierte mit der Unterstützung des Büros des Sonderbeauftragten und Koordinators für die Bekämpfung des Menschenhandels der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) das Projekt «Financial Intelligence Against Human Trafficking».

Dieses Projekt verfolgte folgende Ziele:

- Erstellung eines Guides zur Sensibilisierung der Finanzintermediäre
- Stärkung der Zusammenarbeit und Optimierung der operativen Abläufe zwischen der MROS und den anderen relevanten Akteuren durch den Aufbau einer Multi-Stakeholder-Partnerschaft

Mit dem offiziellen Projektbeginn – einem Runden Tisch am 24. Januar 2024 – übernahm die MROS die Leitung des Projekts. In Zusammenarbeit mit verschiedenen Strafverfolgungs- und Bundesbehörden, Vertretern aus dem Finanzsektor sowie dem Opferschutz wurden Daten und Informationen für den FIAHT-Guide zusammengetragen. So wurden die Weichen für die ebenfalls im Zentrum stehende Intensivierung des Austausches unter den Akteuren gestellt. Am 25. November 2024 fand der Abschlussevent des Projekts FIAHT in Bern statt, an welchem der Inhalt des Guides präsentiert wurde.

FIAHT-Guide[18]

Der Guide bietet klare Ansätze und Instrumente, die Finanzintermediäre sowie Händlerinnen und Händler darin unterstützt, Transaktionen und Verhaltensweisen im Bereich der Schwerstkriminalität zu identifizieren. Dazu gehören:

- **Indikatoren,** die auf Menschenhandel und verwandte Straftaten schliessen lassen.
- **Praktische Beispiele,** die aufzeigen, wie Täter ihre Gewinne verschleiern und wie Finanzintermediäre solche Muster erkennen können.
- **Good Practices,** die Finanzintermediären zeigen, wie sie Verdachtsmeldungen effizient und präzise erstatten können, um die Analysen und nachgelagerten Ermittlungen zu unterstützen.

Im Kampf gegen die Geldwäscherei, deren Vortaten und der organisierten Kriminalität sind solche Sensibilisierungsmassnahmen entscheidend, um die Differenz zwischen der Anzahl der Verdachtsmeldungen und der finanziellen Relevanz dieser Verbrechen zu verringern.

2.5.2 Typologienbericht

Der Präventivauftrag der MROS umfasst die Sensibilisierung der Finanzintermediäre sowie der Händlerinnen und Händler für die Problematik der Geldwäscherei, deren Vortaten, der organisierten Kriminalität und der Terrorismusfinanzierung. Neben den regelmässigen Publikationen wie

[18] Publiziert unter: Publikationen der Meldestelle für Geldwäscherei (MROS).

den Jahresberichten und den Nationalen Risikoanalysen (NRA), veröffentlicht die MROS ebenfalls Newsletters und erarbeitet spezifische Guidelines (z. B. den HAMAS-Alert oder den FIAHT-Guide; vgl. Kap. 2.5.1). Diese Publikationen dienen den Finanzintermediären zur Orientierung, als Leitfaden und als Best Practice.

Als weiteres Sensibilisierungsinstrument lancierte die MROS einen Typologienbericht[19]. Typologien hinsichtlich Geldwäscherei beziehen sich auf die systematische Klassifikation und Analyse von typischen Methoden und Vorgehensweisen, die von Kriminellen genutzt werden, um illegale Gelder in den legalen Wirtschaftskreislauf einzuführen. Diese «Modi operandi» umfassen eine Vielzahl von Techniken, die es den Tätern ermöglichen, die Herkunft des Geldes zu verschleiern und die Einziehung zu vereiteln. Der Typologienbericht unterstützt die Finanzintermediäre darin, mögliche Indikatoren zu erkennen. Die MROS verwendet für die Typologien anonymisierte und vereinfachte Sachverhalte. Diese ermöglichen eine klare Analyse komplexer Zusammenhänge, fördern eine differenzierte Betrachtung und bieten eine hilfreiche Struktur, um wiederkehrende Muster zu erkennen.

Im Mai 2025 veröffentlicht die MROS die ersten Typologien auf ihrer Homepage[20]. Die Sammlung wird laufend ergänzt, richtet sich in erster Linie an Finanzintermediäre sowie Händlerinnen und Händler und wird vorerst ausschliesslich auf Englisch publiziert.

2.5.3 MROS Crypto-Symposium 2.0

Wie bereits im Vorjahr führte die Meldestelle Ende Oktober 2024 ein «Crypto-Symposium» durch. Der Fokus des ersten Symposiums 2023 lag auf den Herausforderungen bei der Nachverfolgung von Kryptowährungen sowie bei der Aufdeckung von Straftaten in Zusammenhang mit Kryptowährungen. 2024 standen die konkreten Gefahren und Missbrauchsmöglichkeiten im Umgang mit Kryptowährungen im Zentrum. Rund 270 Teilnehmende aus der Finanz- und Beratungsindustrie sowie aus dem öffentlichen Sektor nahmen teil. Als Referierende traten verschiedene Vertreterinnen und Vertreter von nationalen und internationalen Behörden sowie dem Privatsektor auf.

Thematisiert wurden unterschiedliche Kriminalitätsfelder, bei denen Kryptowährungen missbraucht werden. Das Spektrum reichte von Cyberkriminalität, Sanktionsumgehung, Asset Recovery und Glücksspiel, bis hin zu Betrug und der unrechtmässigen Verwendung durch private Sicherheitsunternehmen. Neben einer Einordnung von Virtual Assets in Bezug zur bevorstehenden FATF-Länderprüfung, teilten mehrere Behörden ihre Erfahrungen im Umgang mit digitaler Kriminalität und berichteten über die Bekämpfung von Investmentbetrug. Ein weiteres Thema war der Missbrauch von Kryptowährungen zur Finanzierung von Kriegen und Söldnertruppen. Es wurde darauf hingewiesen, dass über Plattformen wie z. B. Telegram Spendenaufrufe zur Finanzierung militärischer Aktivitäten organisiert werden, was neue Herausforderungen für die Strafverfolgung mit sich bringt.

Zusammenfassend zeigt sich die Notwendigkeit einer verstärkten nationalen und internationalen Zusammenarbeit sowie der gezielte Einsatz technischer Instrumente, um der wachsenden Krypto-Kriminalität entgegenzuwirken.[21]

2.5.4 Chinese Underground Round Table

«Hawala» im mittleren Osten und Afrika, «Hundi» in Südasien, «Fei Ch'ein» und «Daigou» in China: Das System des «Underground Banking» ist nicht neu; es existiert, seit es grenzüberschreitenden Handel gibt. Die Systeme funktionieren abseits des gängigen Bankensystems ohne staatliche Zulassung und Aufsicht. Belege, Kontodaten und Bankkonten sucht man vergebens. Die Transaktion erfolgt schnell, günstig und anonym. Genau dies macht das System für die Verschleierung und das Verschieben von kriminellen Geldern und für die Terrorismusfinanzierung so interessant. Dennoch gelingt es Strafverfolgungsbehörden immer wieder, Systeme und Geldströme aufzudecken. Der Austausch von Erkenntnissen aus solchen Erfolgen und Analysen sowie bewährten Vorgehensweisen

[19] Wird zu einem späteren Zeitpunkt in eine Datenbank überführt.

[20] Mehr unter: Publikationen der Meldestelle für Geldwäscherei (MROS).

[21] Medienmitteilung fedpol vom 29. Oktober 2024, «MROS Crypto-Symposium 2.0: Gemeinsam gegen den Missbrauch von Kryptowährungen».

ist deshalb sehr wichtig. Die MROS organisierte den ersten schweizweiten Runden Tisch zum chinesischen Untergrund-Banksystem. Das Treffen richtete sich primär an Schweizer und internationale Strafverfolgungsbehörden und Geldwäschereimeldestellen, welche aktiv zur Bekämpfung der organisierten Kriminalität beitragen. Am Runden Tisch vertreten waren fedpol, Europol sowie Strafverfolgungsbehörden und FIUs mehrerer europäischer Länder.[22]

[22] Medienmitteilung fedpol vom 31. Oktober 2024, «Erster Runder Tisch zur Bekämpfung von Untergrundbanken».

3 Jahresstatistik der Meldestelle

Die MROS erstellt anonymisierte Statistiken, um Informationen über Geldwäscherei, deren Vortaten, organisierte Kriminalität und Terrorismusfinanzierung während des Geschäftsjahrs[23] auszuwerten. Diese umfassen insbesondere die Verdachtsmeldungen der Finanzintermediäre, Auskunftsbegehren von entsprechenden ausländischen Behörden sowie die Verfahren, die auf die Meldungen folgen (vgl. Art. 23 Abs. 1 MGwV[24]).

3.1 Gesamtübersicht 2024

- Die Anzahl der eingereichten **Verdachtsmeldungen** hat im Jahr 2024 weiter deutlich zugenommen: Die MROS erhielt 2024 **15 141** Verdachtsmeldungen, was rund 59 Meldungen pro Werktag entspricht. Im Vergleich zu 2023 (11 876) entspricht dies einer Zunahme von 27,5%. Seit der Einführung des Informationssystems goAML im Januar 2020 hat sich das Meldevolumen knapp verdreifacht.
- **92,3%** der Verdachtsmeldungen stammen von Finanzintermediären aus dem **Bankensektor** (Durchschnitt 2015 – 2024: 90,1%).
- **1016 Informationsanfragen nach Artikel 11*a* GwG** übermittelte die MROS im 2024 an die Finanzintermediäre.
- Im Vergleich zum Vorjahr übermittelte die Meldestelle 2024 **+20,4%** mehr **Anzeigen an die Strafverfolgungsbehörden**[25]. Die MROS übermittelt den Strafverfolgungsbehörden jeweils einen Analysebericht mit den relevanten Informationen. Diese können Informationen aus mehreren Verdachtsmeldungen, die nicht zwingend im selben Jahr bei der MROS eingegangen sind und Informationen von verschiedenen in- und ausländischen Behörden beinhalten. 2024 übermittelte die MROS im Schnitt 1,9 Verdachtsmeldungen pro Anzeige an die Strafverfolgungsbehörden. Auch hier zeigt sich eine stetige Zunahme der durchschnittlichen Anzahl der übermittelten Verdachtsmeldungen pro Anzeige.[26] Rund jede fünfte Übermittlung (18,9%) beinhaltete zudem Informationen basierend auf einer oder mehreren Anfragen der MROS nach Artikel 11*a* GwG bei meldenden Finanzintermediären oder Drittintermediären.
- Der Informationsaustausch zwischen der MROS und den Schweizer Behörden nimmt zu. Im Vergleich zum Vorjahr nahm die **spontane Informationsübermittlung der MROS** an andere **Schweizer Behörden** um 79% zu. Rückläufig waren hingegen die Informationsanfragen (447, was einem Minus von 35,8% gegenüber dem Vorjahr entspricht) und Spontaninformationen (106, was einem Minus von 10,9% entspricht) von anderen Schweizer Behörden an die MROS.
- Der **Informationsaustausch mit ausländischen Meldestellen (FIU)** nimmt ebenfalls konstant zu. Im Jahr 2024 gingen bei der MROS 780 Anfragen von 96 ausländischen Meldestellen und 751 Spontaninformationen aus 45 Ländern ein.

[23] Geschäftsjahr: 1. Januar bis 31. Dezember des jeweiligen Jahres.
[24] Verordnung über die Meldestelle für Geldwäscherei (MGwV), SR 955.23.
[25] 2024: 1043; 2023: 866.
[26] 2022:1,4; 2023: 1,8.

3.2 Verdachtsmeldungen

Im Jahr 2024 gingen bei der MROS pro Werktag im Schnitt 59 Verdachtsmeldungen ein. Insgesamt erhielt die MROS 2024 15 141 Meldungen von Finanzintermediären sowie Händlerinnen und Händlern, was einer erneuten Zunahme von 27,5% gegenüber dem Vorjahr entspricht. Seit der Einführung des Informationssystems goAML im Jahr 2020 hat sich die Anzahl der übermittelten Verdachtsmeldungen damit knapp verdreifacht (vgl. Abbildung 4). [27]

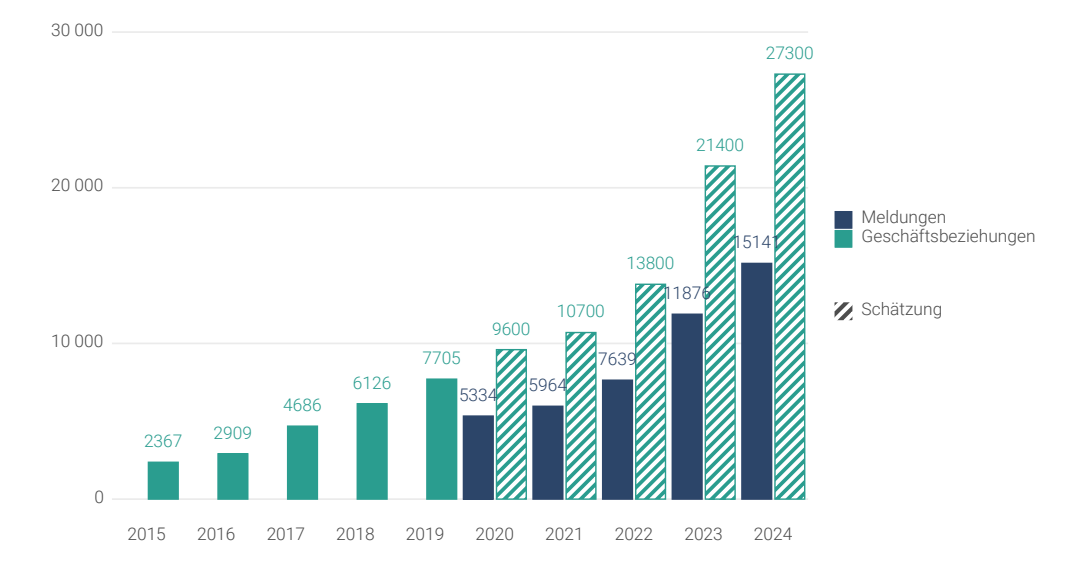
Wie Abbildung 4 zeigt, hat sich die Anzahl der jährlich gemeldeten Geschäftsbeziehungen seit 2015 knapp verzwölffacht. 2015 wurden der MROS insgesamt 2367 verdächtige Geschäftsbeziehungen gemeldet; 2024 waren es rund 27 300. Diese Zunahme hat mehrere Gründe: Zum einen sind die Sensibilität und das Bewusstsein der Finanzintermediäre für die Geldwäschereithematik gewachsen. Zum anderen spielen die rechtlichen Anpassungen sowie die Fortschritte in der Digitalisierung (z. B. verbesserte Tools beim Transaktionsmonitoring und in der internen Analyse) eine zentrale Rolle.[28]

3.3 Verdachtsmeldungen nach Branche der Meldepflichtigen

92,3% der Verdachtsmeldungen stammen von Finanzintermediären aus dem Bankensektor. Das Meldeverhalten dieser Finanzintermediäre beeinflusst die Anzahl und Art der Meldungen, die bei der MROS eingehen massgeblich. Die Verteilung der Verdachtsmeldungen auf die Meldepflichtigen hat sich seit Einführung des Informationssystems goAML kaum verändert (vgl. Tabelle 1).

Seit 2024 werden Virtual Asset Service Provider (VASP) und FinTech-Anbieter als eigene Kategorie erfasst. Im Jahr 2024 reichten VASP und FinTech-Finanzintermediäre 227 Verdachtsmeldungen bei der MROS ein (1,5%).

Abbildung 4: Anzahl gemeldete Geschäftsbeziehungen und Verdachtsmeldungen
2015 – 2024



[27] Mit der Einführung von goAML wurde die Zählweise der Verdachtsfälle angepasst. Um dennoch einen Vergleich mit den Vorjahren zu ermöglichen, wird in Abbildung 4 die durchschnittliche Anzahl gemeldeter Geschäftsbeziehungen pro Verdachtsmeldung im Geschäftsjahr 2019 angewendet. Diese beläuft sich auf 1,8. Das bedeutet, dass die 15 141 Verdachtsmeldungen im Jahr 2024 geschätzt rund 27 300 Geschäftsbeziehungen entsprechen.

[28] Vgl. Ausführungen im Jahresbericht MROS 2023, Kap. 2.1.

Tabelle 1: Verdachtsmeldungen nach Branche, 2015 – 2024[29]

Branche	2015[A]	2016	2017[A]	2018[A]	2019[A]	2020[B]	2021[B]	2022[B]	2023[B]	2024[B]	2024 in absoluten Zahlen	Durchschnitt 2015 – 2024
Banken	91,3%	86%	91%	88,8%	89,9%	89,5%	90,0%	91,6%	90,5%	92,3%	13 973	90,1%
Zahlungsverkehrsdienstleister	2,4%	4,4%	3,1%	4,4%	4,0%	3,5%	2,5%	2,0%	2,8%	2,2%	339	3,1%
Kreditkartenanbieter	0,5%	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	1,6%	235	1,2%
VASP / FinTech										1,5%	227	
Vermögensverwaltung	1,9%	2,2%	1,9%	1,0%	0,9%	0,8%	1%	0,6%	0,8%	0,9%	137	1,2%
Casinos	0,1%	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	0,3%	47	0,5%
Kredit-, Leasing-, Factoring- und Forfaitierungsgeschäfte	0,3%	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	0,2%	37	0,3%
Wertpapierhäuser	0,1%	0,1%	0,3%	0,1%	0,3%	0%	0,2%	0,1%	0,2%	0,2%	32	0,2%
Treuhänder	2%	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	0,2%	30	0,8%
Übrige Finanzintermediäre	0,2%	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2%	0,2%	24	1,3%
Rohwaren- und Edelmetallhandel	0,3%	0,1%	0,2%	0%	0,3%	0,2%	0,5%	0,3%	0,3%	0,2%	23	0,2%
Versicherungen	0,5%	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	0,2%	23	0,7%
Geldwechsel/Change	0%	0%	0%	0%	0%	0,1%	0,1%	0,3%	0,6%	0%	5	0,1%
Rechtsanwälte und Notare	0,3%	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0%	0,1%	0%	5	0,1%
SRO	0%	0%	0%	0%	0,1%	0%	0%	0%	0,1%	0%	4	0%
Behörden (FINMA/ESBK/GESPA)	0%	0%	0%	0%	0%	0%	0,1%	0%	0%	0%	0	0%
Devisenhandel	0%	0,1%	0%	0%	0,3%	0%	0%	0%	0%	0%	0	0%
Trustees	0%	0%	0%	0%	0%	0,1%	0,1%	0%	0%	0%	0	0%
Vertriebsträger von Anlagefonds	0%	0%	0,1%	0%	0%	0%	0%	0%	0%	0%	0	0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**15 141**	**100,0%**

[A] Nach alter Zählweise (Geschäftsbeziehung)

[B] Nach neuer Zählweise (Meldungen)

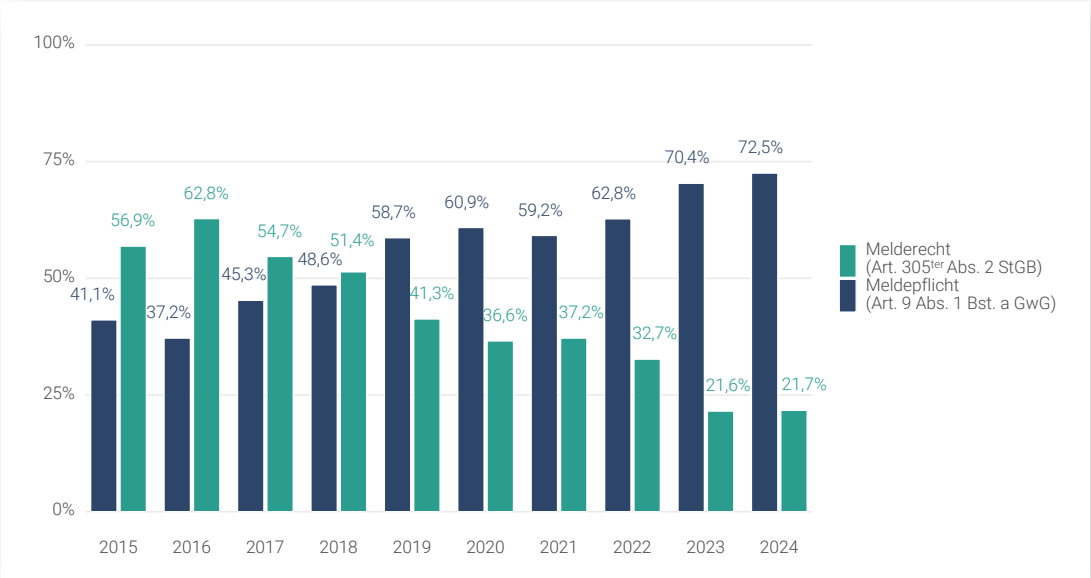
[29] Die absoluten Zahlen für die Jahre 2014 – 2023 sind in den Jahresberichten der MROS der entsprechenden Jahre veröffentlicht.

3.4 Rechtsgrundlage der Meldungen

Die Rechtsgrundlage für eine Verdachtsmeldung ist abhängig vom Verdachtsgrad. Liegt ein begründeter Verdacht vor, haben Finanzintermediäre nach Artikel 9 Absatz 1 Buchstabe a GwG[30] die Pflicht, dies der MROS zu melden. Bei einfachem Verdacht können sie sich auf das Melderecht nach Artikel 305ter Absatz 2 StGB[31] stützen. 2024 erstatteten die GwG-Unterstellten in 72,5% der Fälle eine Verdachtsmeldung aufgrund der Meldepflicht (Art. 9 Abs. 1 Bst. a GwG, vgl. Abbildung 5). Das Melderecht nach Artikel 305ter Absatz 2 StGB wendeten sie bei 21,7% der eingereichten Verdachtsmeldungen an. In 5,6% der Fälle meldeten die Finanzintermediäre zudem, 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).[32]

Seit 2018 gewinnt die Meldepflicht gegenüber dem Melderecht stetig an Gewicht, mit einem markanten Gewinn im 2023 (vgl. Jahresbericht MROS 2023, Kap. 4.4). Nach einem stetigen Bedeutungszuwachs der Meldepflicht in den vergangenen Jahren, zeigt sich in der diesjährigen Statistik erstmals eine gewisse Konsolidierung des Verhältnisses zwischen Meldepflicht und Melderecht. Während der Gebrauch der Meldepflicht bei einer bestehenden Geschäftsbeziehung gegenüber dem Vorjahr um 2,1% zugenommen hat, verzeichnet das Melderecht eine marginale Zunahme von +0,1%. Ein Rückgang von −2,3% erfahren die Meldungen von Finanzintermediären bei einem Abbruch der Verhandlungen zur Aufnahme einer neuen Geschäftsbeziehung nach Artikel 9 Absatz 1 Buchstabe b GwG.

Abbildung 5: Meldungen bei bestehender Geschäftsbeziehung nach Rechtsgrundlage
2015 – 2024



[30] Art. 9 Abs. 1 Bst. a GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Artikel 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 Artikel 260ter oder 305bis StGB stehen, (2.) aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Artikel 305bis Ziffer 1bis StGB herrühren, (3.) der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen, oder (4.) der Terrorismusfinanzierung (Art. 260quinquies Abs. 1 StGB) dienen.

[31] Art. 305ter Abs. 2 StGB: Die von Absatz 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 Artikel 305bis Ziffer 1bis herrühren.

[32] Art. 9 Abs. 1 Bst. b GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Artikel 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.

3.5 Vortaten

Finanzintermediäre geben bei einer Meldung jeweils an, welche Vortat(en) sie vermuten. Im Laufe der letzten Jahre werden rund zehn verschiedene Vortaten am häufigsten genannt (vgl. Abbildung 6).[33] Die Vortat, die von den Finanzintermediären am meisten erwähnt wird, ist Betrug. Dieser wird 2024 in 59,4% aller Meldungen angegeben; entweder allein oder in Kombination mit anderen Delikten (im Zeitraum 2020 – 2023 betrug dieser Anteil 57,2%). Deutlich seltener werden andere Vortaten wie Urkundenfälschung (7,1%; im Zeitraum 2020 – 2023: 12,1%) oder Veruntreuung (4,1%; im Zeitraum 2020 – 2023: 6,1%) genannt.

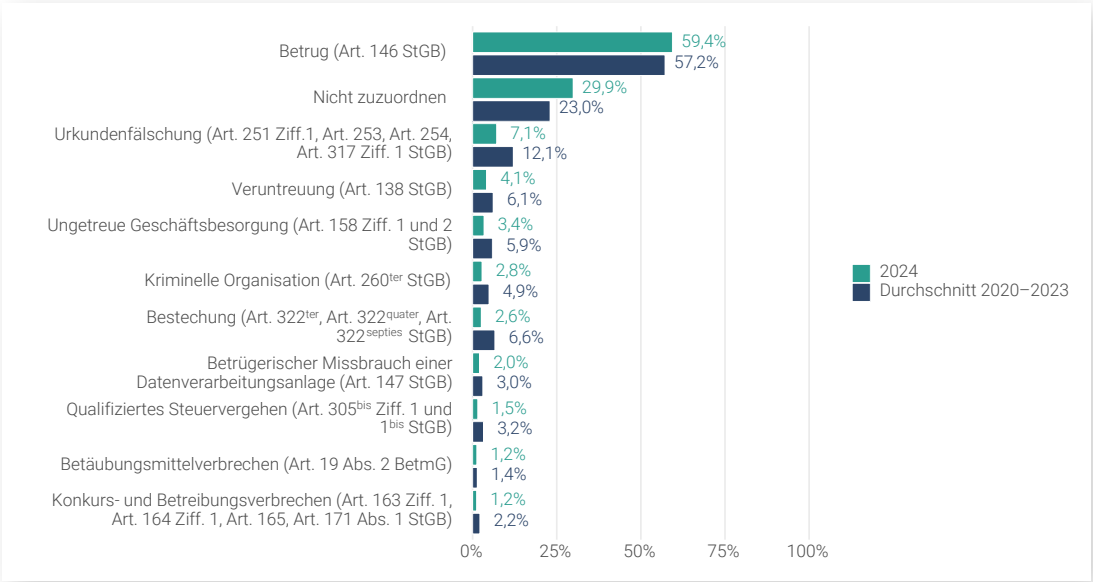
Bei den Angaben der Finanzintermediäre zu den vermuteten Vortaten handelt es sich um eine erste wichtige Qualifikation aufgrund der von den Finanzintermediären getätigten Abklärungen. Die vorstehende Abbildung spiegelt wider, welche Straftaten die Finanzintermediäre beim Einreichen der Verdachtsmeldung vermuten. Eine Analyse der MROS kann den Verdacht auf eine andere Straftat ergeben.[34]

Im Jahr 2024 geben die Meldepflichtigen bei nahezu jeder dritten Verdachtsmeldung (29,9%) an, keine Vortat zuordnen zu können. Diese Tendenz manifestierte sich im Verlaufe der Jahre zusehends und hat auch im Berichtsjahr weiter zugenommen. Die Tatsache, dass rund ein Drittel der Verdachtsmeldungen ohne Angabe einer Vortat bei der MROS eingereicht werden, hat weitreichende Folgen. Die MROS muss zusätzliche Ressourcen für weitere Abklärungen zur Vortat einsetzen.

3.6 Verdachtsauslösende Elemente

In der Regel reichen die Finanzintermediäre eine Verdachtsmeldung an die MROS als Ergebnis ihres Transaktionsmonitorings ein (2024: 29,6%; 2020 – 2023: 32,0%; vgl. Abbildung 7).[35] Als weitere verdachtsauslösende Elemente folgen mit 26,9% die Informationen Dritter (externe Informations-

Abbildung 6: Häufigkeit der vermuteten Vortaten
2020 – 2024, Mehrfachnennungen möglich

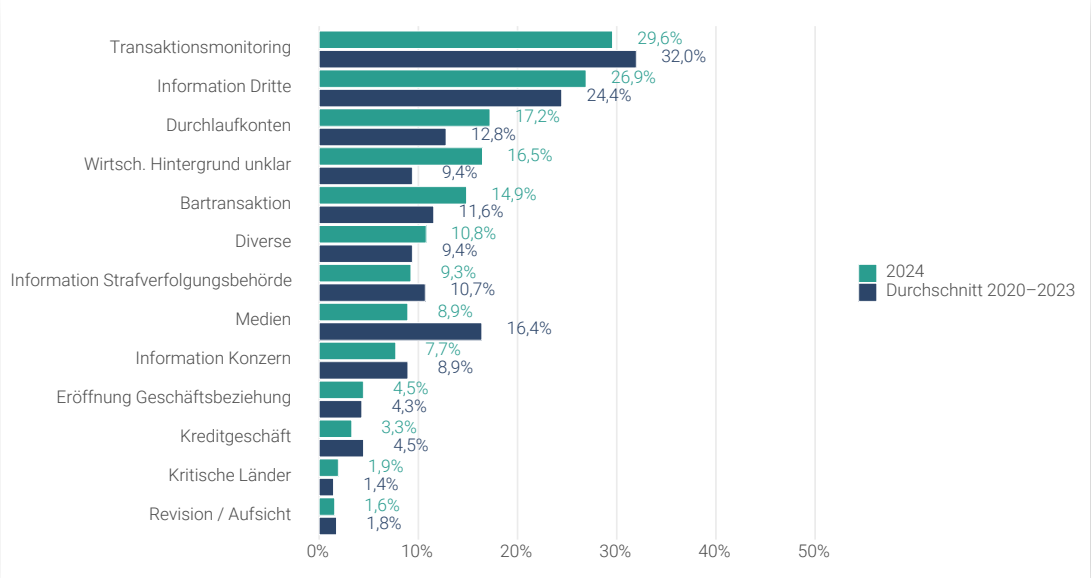


[33] Mit der Einführung des goAML 2020 sind Mehrfachnennung möglich. Einen Vergleich mit den Statistiken vor 2020 ist deshalb nicht möglich.

[34] 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.

[35] Gegenüber den Jahren vor 2020 können die Finanzintermediäre 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.

Abbildung 7: Wichtige Verdachtsauslöser
2020 – 2024, Mehrfachnennungen möglich



quellen) und Durchlaufkonten mit 17,2%. Im Vergleich zu den Vorjahren melden die Finanzintermediäre im Jahr 2024 bedeutend häufiger, dass der wirtschaftliche Hintergrund der Geschäftsbeziehung unklar sei (16,5%; 2020 – 2023: 9,4%).

3.7 Anzeigen an die Strafverfolgungsbehörden

2024 übermittelte die MROS gestützt auf Artikel 23 Absatz 4 GwG 1043 Anzeigen an die Strafverfolgungsbehörden. Dies entspricht einer Zunahme von +20,4% gegenüber dem Vorjahr (2023: 866). In den vergangenen Jahren haben sich die von der MROS übermittelten Anzeigen an die Strafverfolgungsbehörden inhaltlich zunehmend erweitert: 2022 enthielt eine Anzeige im Durchschnitt 1,4 Verdachtsmeldungen; 2024 waren es im Durchschnitt 1,9 Verdachtsmeldungen.

Die 1043 übermittelten Anzeigen enthalten Informationen aus:

- 1481 im Jahr 2024 eingegangenen Meldungen
- 432 im Jahr 2023 eingegangenen Meldungen
- 32 im Jahr 2022 eingegangenen Meldungen
- 13 im Jahr 2021 eingegangenen Meldungen
- fünf im Jahr 2020 eingegangenen Meldungen
- zwei vor dem Jahr 2020 gemeldeten Geschäftsbeziehungen

Davon übermittelte die MROS 89,7% der Anzeigen an die kantonalen Staatsanwaltschaften und 10,3% gingen an die Bundesanwaltschaft.

Wie bereits in den vergangenen Jahren konzentrierte sich mehr als die Hälfte der Anzeigen auf eine begrenzte Zahl weniger kantonaler Staatsanwaltschaften und an die Bundesanwaltschaft: Anzeigen an die Staatsanwaltschaften der Kantone Zürich (17,9%), Waadt (12,4%) und Genf (10,2%) sowie an die Bundesanwaltschaft (10,3%) machen rund die Hälfte aller von der MROS übermittelten Anzeigen aus (vgl. Tabelle 2).

Im Jahr 2024 übermittelte die MROS den Strafverfolgungsbehörden knapp 60% der Anzeigen aufgrund des begründeten Verdachts, dass die Vermögenswerte aus einem Betrug herrühren könnten. In einem Fünftel der Übermittlungen zeigte sie den Straftatbestand der Geldwäscherei an sich an (vgl. Abbildung 8). Dies beispielsweise, wenn der Beschuldigte der Vortat nicht mit derjenigen Person übereinstimmt, welche die Geldwäschereihandlung vornimmt.

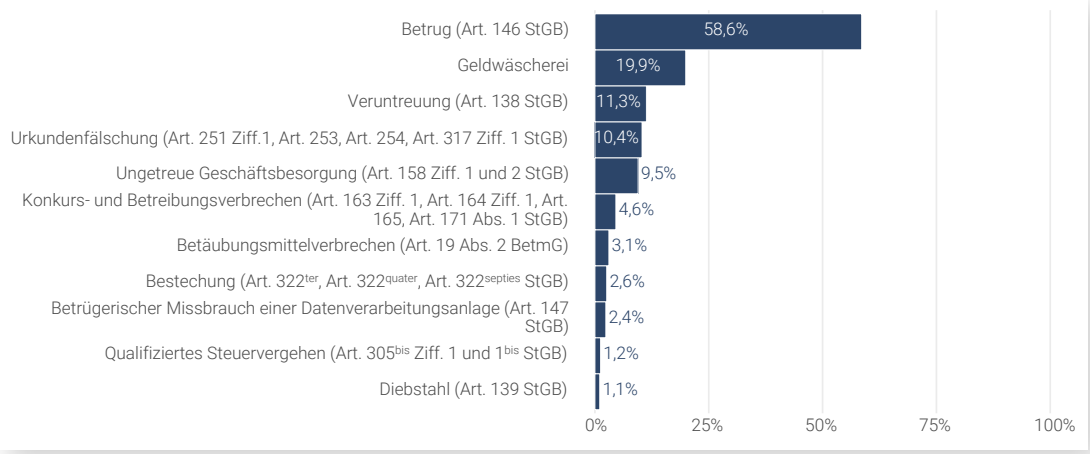
3.8 Rückmeldungen der Strafbehörden

Gemäss Artikel 29*a* GwG melden die Strafbehörden der MROS sämtliche hängigen Verfahren

Tabelle 2: Übermittelte Anzeigen nach Strafverfolgungsbehörden 2020 – 2024

Behörde	2020	2021	2022	2023	2024	2024 in absoluten Zahlen	Durchschnitt 2020 – 2024
Zürich	18,9%	21,1%	20,4%	16,3%	17,9%	187	18,9%
Waadt	11,1%	11,6%	10,6%	8,3%	12,4%	129	10,8%
Bundesanwaltschaft	**9,0%**	**9,1%**	**6,4%**	**13,0%**	**10,3%**	**107**	**9,6%**
Genf	11,5%	11,3%	11,6%	17,6%	10,2%	106	12,4%
Bern	7,5%	6,7%	6,9%	6,5%	7,7%	80	7,1%
Aargau	5,3%	5,2%	6,7%	4,2%	5,7%	59	5,4%
Tessin	5,0%	4,8%	3,6%	4,6%	5,5%	57	4,7%
St. Gallen	3,5%	4,0%	6,3%	5,3%	5,3%	55	4,9%
Luzern	3,5%	2,9%	2,6%	2,5%	3,9%	41	3,1%
Basel-Stadt	2,6%	2,3%	2,3%	1,8%	3,2%	33	2,4%
Wallis	2,7%	2,4%	3,0%	2,2%	2,9%	30	2,6%
Basel-Landschaft	2,1%	1,7%	2,3%	1,8%	2,2%	23	2,0%
Freiburg	2,7%	3,1%	2,1%	1,3%	2,1%	22	2,3%
Solothurn	1,9%	2,0%	2,1%	1,4%	2,1%	22	1,9%
Thurgau	3,0%	2,1%	2,6%	3,2%	1,7%	18	2,5%
Schwyz	1,0%	1,1%	1,9%	2,1%	1,5%	16	1,5%
Zug	2,5%	2,6%	2,2%	2,2%	1,2%	12	2,1%
Graubünden	1,5%	1,0%	1,1%	0,6%	1,1%	11	1,1%
Neuenburg	2,3%	1,9%	1,7%	1,3%	1,0%	10	1,6%
Schaffhausen	0,5%	0,5%	0,6%	0,7%	0,6%	6	0,6%
Appenzell Ausserrhoden	0,6%	0,8%	1,3%	0,9%	0,5%	5	0,8%
Jura	0,3%	1,0%	0,2%	0,7%	0,4%	4	0,5%
Appenzell Innerrhoden	0,0%	0,1%	0,2%	0,2%	0,3%	3	0,2%
Nidwalden	0,3%	0,4%	0,6%	0,6%	0,3%	3	0,4%
Glarus	0,2%	0,1%	0,4%	0,6%	0,2%	2	0,3%
Obwalden	0,2%	0,1%	0,2%	0,0%	0,2%	2	0,1%
Uri	0,3%	0,1%	0,2%	0,1%	0,0%	0	0,1%
Total	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100%**	**1043**	**100,0%**

Abbildung 8: Häufigkeit der angezeigten Straftatbestände an die Strafverfolgungsbehörden, 2024
Mehrfachnennungen möglich



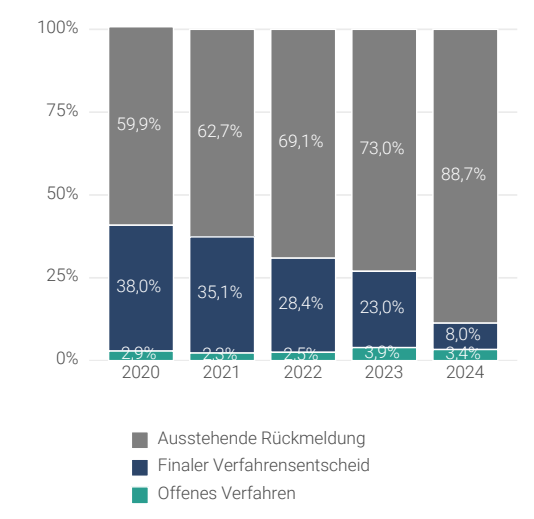
insbesondere zu Geldwäscherei, kriminellen und terroristischen Organisationen sowie Finanzierung des Terrorismus.[36] Zudem informieren sie die MROS unverzüglich über Verfügungen, die sie aufgrund einer Anzeige der Meldestelle erlassen haben.[37] Diese Rückmeldungen sind für den Auftrag der MROS, die Strafverfolgungsbehörden bestmöglich zu unterstützen, entscheidend.

Die Statistiken des Jahresberichts 2023 verdeutlichen, dass bei einem Grossteil der Anzeigen noch keine Rückmeldungen vorliegen, was auf die zeitintensive Bearbeitung durch die Strafbehörden zurückzuführen ist.[38] Betrachtet man ausschliesslich jene Anzeigen, deren Übermittlung per Jahresende 2024 mehr als zwölf Monate zurückliegen (Zeitraum 2020 – 2023), so ergibt sich, dass am 31. Dezember 2024 bei rund zwei Dritteln der übermittelten Fälle (64,3%) noch keine Informationen zum Verfahrensstand vorliegen.

Die Strafbehörden meldeten der MROS 2024 82 Strafbefehle und 48 Urteile, die im Zusammenhang mit Anzeigen der MROS erlassen wurden, sowie 262 Nichtanhandnahmen oder Einstellungsverfügungen.

In Anbetracht der überwiegenden Anzahl an ausstehenden Rückmeldungen ist es der MROS nicht möglich, Erkenntnisse über das Verhältnis von Urteil sowie Nichtanhandnahme- und Einstellungsverfügung ziehen. Die MROS unternimmt deshalb weitere Anstrengungen und sucht Lösungen mit den Strafbehörden, um die gesetzlich vorgesehenen Rückmeldungen im Zusammenhang mit den Artikeln 260ter, 260^{quinquies} Absatz 1, 305bis und 305ter Absatz 1 StGB zu erhalten.

Abbildung 9: Rückmeldungen und Stand der im jeweiligen Jahr übermittelten Anzeigen
2020 – 2024



3.9 Terrorismusfinanzierung

2024 erhielt die MROS 106 Meldungen wegen Verdacht auf Terrorismusfinanzierung und / oder wegen Verstoss gegen das Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen[39]. Dies entspricht 0,7% aller eingegangenen Meldungen. Die meisten davon werden zusätzlich mit anderen Vortaten in Verbindung gebracht. Zu den häufigsten weiteren Verdachtsgründen zählen:

- Zugehörigkeit zu kriminellen und terroristischen Organisationen[40] (25 Nennungen)
- Betrug[41] (9 Nennungen)
- Verstoss gegen das Embargogesetz[42] (4 Nennungen)
- Verstoss gegen das Betäubungsmittelgesetz[43] (3 Nennungen)

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

[37] Art. 29*a* Abs. 2 GwG.

[38] Vgl. Jahresbericht MROS 2023, S. 26 f.

[39] Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen, SR 122, vollständige Aufhebung per 1. Dezember 2022.

[40] Art. 260ter StGB.

[41] Art. 146 StGB.

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

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

- Anwerbung, Ausbildung und Reisen im Hinblick auf eine terroristische Straftat[44] (3 Nennungen)
- Ungetreue Geschäftsbesorgung (3 Nennungen)[45]

Die Meldungen mit Verdacht auf Terrorismusfinanzierung stammen überwiegend von Banken (76 Meldungen); weitere 15 Meldungen von Zahlungsverkehrsdienstleistern.

Als Verdachtsauslöser für die Meldung nennen die Finanzintermediäre 2024 am häufigsten:

- Presseberichte (36 Nennungen)
- Transaktionsmonitoring (33 Nennungen)
- Informationen von Dritten (26 Nennungen)
- Bartransaktionen (24 Nennungen)
- Unklarheiten bezüglich wirtschaftlichen Hintergrunds (19 Nennungen)

Die 106 im Verlauf des Jahres 2024 eingegangenen Meldungen führten bis 31. Dezember 2024 zu zehn Anzeigen zuhanden der zuständigen Strafverfolgungsbehörden.

3.10 Organisierte Kriminalität

Von den 15 141 Meldungen, die im Jahr 2024 bei der MROS eingingen, äusserte der Finanzintermediär in 424 Fällen (2,8%) den Verdacht einer Verbindung zu kriminellen Organisationen. Die überwiegende Mehrheit dieser Verdachtsmeldungen stammen aus dem Bankensektor (90,5%). Auslöser für die Verdachtsmeldung waren nach Angaben der Finanzintermediäre hauptsächlich Informationen aus Medien (28,5%) und / oder ein Transaktionsmonitoring (17,2%; vgl. Tabelle 3).

Zusätzlich zur vermuteten Verbindung zu einer kriminellen Organisation nannten die Finanzintermediäre als weitere mögliche Vortat häufig Betrug (42,9%) und / oder Bestechung (8,5%). Die 424 Verdachtsmeldungen im Berichtsjahr führten zu 33 Anzeigen an die zuständigen Strafverfolgungsbehörden.

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

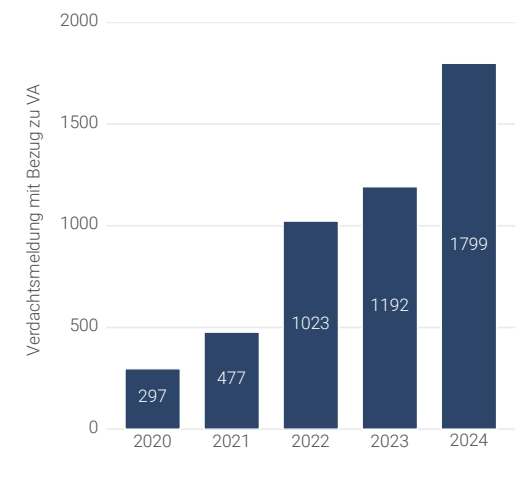
Verdachtsauslöser (Mehrfachnennungen möglich, Häufigkeitsauswahl)	Anzahl Nennungen	in % an Total aller Meldungen
Medien	121	28,5%
Transaktionsmonitoring	73	17,2%
Wirtsch. Hintergrund unklar	59	13,9%
Information Dritte	54	12,7%
Bartransaktion	52	12,3%
Eröffnung Geschäftsbeziehung	36	8,5%
Information Strafverfolgungsbehörde	34	8,0%
Durchlaufkonten	34	8,0%
Information Konzern	29	6,8%
Revision / Aufsicht	20	4,7%

[44] Art. 260^{sexies} StGB.
[45] Art. 158 Ziff. 1 und 2 StGB.

3.11 Verdachtsmeldungen mit Bezug zu virtuellen Währungen

2024 liessen sich 1799 Verdachtsmeldungen identifizieren, die einen Bezug zu virtuellen Währungen aufweisen (Virtual Assets [VA][46]; vgl. Abbildung 10), was wiederum einer Zunahme gegenüber dem Vorjahr entspricht.[47] 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, bergen Kryptowährungen erhöhte Risiken.[48]

Abbildung 10: Anzahl Meldungen mit einem Bezug zu virtuellen Währungen (VA)
2020 – 2024



Seit Frühjahr 2024 erfasst die MROS Finanzintermediäre, die sich aufgrund ihrer Haupttätigkeit zu Anbietern von virtuellen Vermögenswerten zählen (VASP), unter einer eigenen Kategorie.[49] Damit sind Aussagen über das Meldeverhalte dieser Kategorie von Finanzintermediären möglich (vgl. Tabelle 1). Bis zum 31. Dezember 2024 haben sich 30 Finanzintermediäre in der Kategorie VASP/FinTech in goAML registriert.

3.12 Herausgabe von Informationen nach Artikel 11*a* GwG

2024 stellte die MROS den Finanzintermediären 1016 Informationsanfragen auf Basis von Artikel 11*a* GwG. Seit 2021 nahm die Zahl der Anfragen stetig zu; 2024 verzeichnete die MROS einen leichten Rückgang, zurück auf das Niveau von 2021 (vgl. Abbildung 11). Von den 1016 Informationsanfragen richtete die MROS am häufigsten Anfragen an sogenannte Drittintermediäre (40,7%, Art. 11*a* Abs. 2 GwG[50]), die neben dem meldenden Finanzintermediär an einer Transaktion oder einer Geschäftsbeziehung beteiligt sind oder waren. Jede vierte Informationsanfrage ging an die Finanzintermediäre der ursprünglichen Verdachtsmeldungen (24,8%, Art. 11*a* Abs. 1 GwG[51]).

Rund ein Drittel der Informationsanfragen richtete die MROS dagegen an einen Finanzintermediär gestützt auf die Analyse von Informationen einer

[46] 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.

[47] 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.

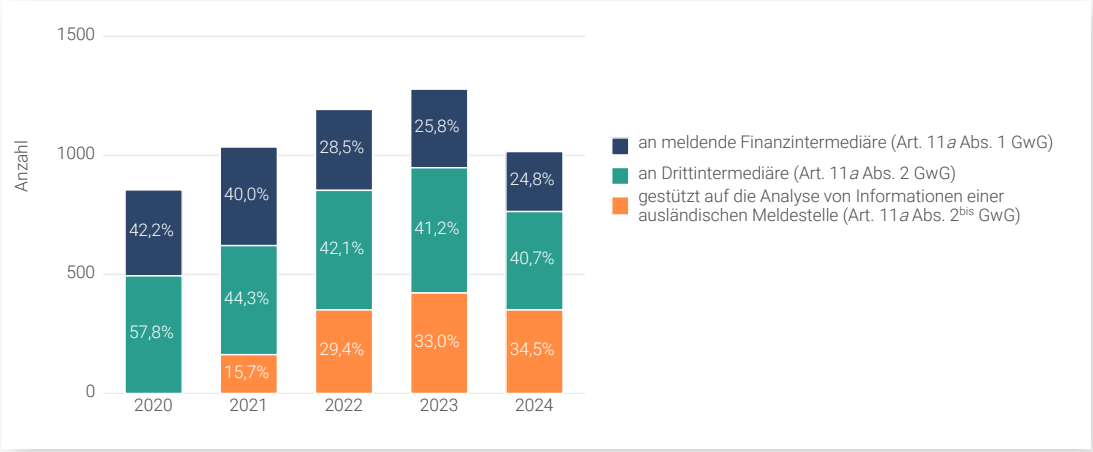
[48] National Risk Assessment (NRA) – Bericht Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, Januar 2024.

[49] 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.

[50] Art. 11*a* 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.

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

Abbildung 11: Aufforderung zur Herausgabe von Informationen nach Artikel 11a GwG
2020 – 2024



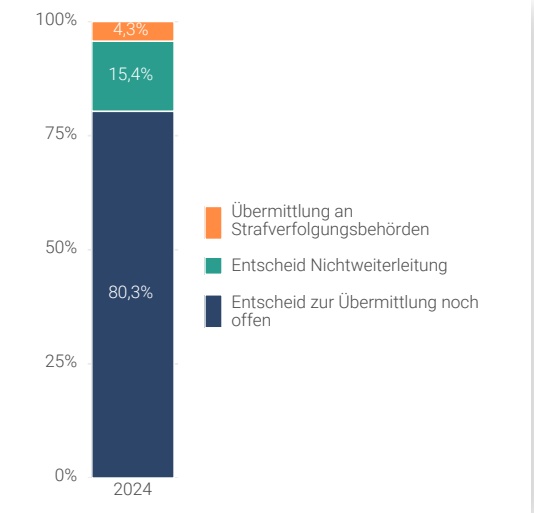
ausländischen Meldestelle (34,5%, Art. 11*a* Abs. 2bis GwG[52]). Seit der Einführung von Artikel 11*a* Absatz 2bis GwG im 2021 gewannen diese Anfragen gegenüber den anderen Anfragen nach Artikel 11*a* GwG zunehmend an Bedeutung (+1,5% gegenüber Vorjahr).

3.13 Abbruchsmeldungen nach Artikel 9*b* GwG

Gestützt auf Artikel 9*b* GwG[53] können Finanzintermediäre seit dem 1. Januar 2023 eine Geschäftsbeziehung 40 Arbeitstage, nachdem sie sie der MROS gemeldet haben, abbrechen – insofern sie nicht über eine Übermittlung an die Strafverfolgungsbehörden informiert wurden. Den Abbruch der Geschäftsbeziehung hat der Finanzintermediär der MROS unmittelbar zu melden.[54]

2024 hat die MROS 7118 Abbruchsmeldungen erhalten; dies sind knapp dreifach so viele wie im Vorjahr (2023: 2669 Abbruchsmeldungen). 4,3% der Abbruchsmeldungen betreffen Verdachtsmeldungen, die über den Jahresverlauf 2024 an die Strafverfolgungsbehörden weitergeleitet wurden (vgl. Abbildung 12).

Abbildung 12: Stand der Verdachtsmeldungen mit Abbruchsmeldungen
2024



[52] Art. 11*a* Abs. 2bis 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.

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

[54] Art. 9*b* Abs. 3 GwG.

3.14 Informationsaustausch mit ausländischen Meldestellen (FIUs)

Im Kampf gegen die Geldwäscherei und deren Vortaten, die Terrorismusfinanzierung und die organisierte Kriminalität funktioniert der Informationsaustausch zwischen der MROS und ihren ausländischen Partnerbehörden (den FIUs) über die Amtshilfe. Diese Informationen sind für die Analysen der MROS von grosser Bedeutung, da eine Vielzahl der Verdachtsmeldungen der Schweizer Finanzintermediäre einen Auslandsbezug haben.[55]

Während die Zahl der Anfragen der MROS an ausländische FIUs in den letzten Jahren zugenommen hatte, zeigt sich 2024 ein leichter Rückgang. 2024 richtete die MROS 239 Auskunftsersuchen an 56 verschiedene FIUs im Ausland (–14,0% im Vergleich zum Vorjahr). Über den Jahresverlauf gingen bei der MROS 780 Anfragen von 96 ausländischen Meldestellen ein. Die MROS bearbeitete 422 der eingegangenen Anfragen sowie zusätzlich 188 Anfragen aus den Vorjahren.

Ausländische FIUs und die MROS können auch Spontaninformationen austauschen. Es handelt sich um einen Informationsaustausch ohne vorherige Anfrage, sei es aus dem Ausland mit einem Bezug zur Schweiz oder von der MROS an eine ausländische FIU. 2024 erhielt die MROS 751 Spontaninformationen aus 45 Ländern (2023: 726 aus 53 Ländern). Die MROS wiederum versendete 189 Spontaninformationen an 41 ausländische FIUs (2023: 160 an 47 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.[56]

Im aktuellen Berichtsjahr erhielt die MROS 447 Informationsanfragen von 35 Schweizer Behörden zu bestimmten Bankkonten, Personen oder Unternehmen (–35,8%; 2023: 696). Wie bereits in den Vorjahren stammen rund 80% aller Anfragen von polizeilichen Behörden. Die MROS übermittelte in 358 Fällen unaufgefordert Informationen an Schweizer Aufsichts- und andere Behörden (+79,0%; 2023: 200). 2024 gingen zudem 106 Spontaninformationen von inländischen Behörden bei der MROS ein (–12,3%, 2023: 119).

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

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

4 Trends

Das neue Kapitel «Trends» in diesem Jahresbericht ersetzt dasjenige der «Typologien», welche ab Mai 2025 auf der Homepage der MROS publiziert werden (vgl. Kap. 2.5.2). Die Trends bieten eine holistische Sichtweise auf die Feststellungen der MROS zu ausgewählten Themenkreisen. In diesem Jahr liegt der Fokus auf Online-Geldspielen, Kinderpornografie und Virtual Assets sowie dem Hamas-Verbot.

4.1 Online-Geldspiele

Allgemein

Das Streben nach Glück und schnellen Gewinnen ist kein modernes oder kulturspezifisches Phänomen, sondern ein tief verwurzeltes menschliches Verhalten, das auch heute weltweit eine bedeutende Rolle spielt. Es zieht Menschen seit Jahrtausenden in seinen Bann[57] und interpretiert man die Zahlen, so ist der Geldspielmarkt – unabhängig, ob online oder vor Ort – am Wachsen.

Im Jahr 2023 wuchs der globale Geldspielmarkt auf ca. 774 Milliarden USD (ca. 691 Milliarden CHF) an, was im Vergleich zum Jahr 2006 einen deutlichen Anstieg darstellt. Damals lag der Umsatz noch bei rund 70 Milliarden USD (ca. 62 Milliarden CHF).[58] Ein ähnliches Wachstum ist auch in der Schweiz zu beobachten: Zwischen 2017 und 2022 stieg der Umsatz des gesamten Schweizer Geldspielsektors um 13%, wobei der Umsatz von etwa 2,2 Milliarden CHF auf rund 2,5 Milliarden CHF anstieg.[59] Etwa sechs von zehn Personen haben in der Schweiz mindestens einmal im Leben für Geld gespielt.[60] Auch der Online-Geldspielmarkt wächst beträchtlich. Bis ins Jahr 2039 sollen die globalen Umsätze von ca. 85 Mrd. USD (ca. 76 Mrd. CHF) im Jahr 2023 auf ca. 173 Mrd. USD (ca. 155 Mrd. CHF) steigen.[61]

Viele Länder verbinden den rapiden Anstieg der Umsätze, insbesondere durch Online-Geldspielaktivitäten, mit einem markanten Risiko-Anstieg der Geldwäscherei. Die USA[62] beispielsweise beobachten einen Anstieg im Geldwäschereirisiko durch die Zunahme an neuen Anbietern von Online-Spielplattformen. Auch die Nationale Risikoanalyse aus Malta weist auf ein signifikantes Risiko im Bereich des Online-Geldspiels hin, insbesondere mit Blick auf potentiell kriminelle Anbieter.[63]

In Anbetracht der steigenden Geldwäschereirisiken, welche im Ausland beobachtet werden, lohnt sich ein Blick auf die Risikolage in der Schweiz.

Potentielles Geldwäschereirisiko

Das Geldwäschereirisiko kann sich bei einer Spielbank in allen drei Phasen der Geldwäscherei manifestieren (Platzierung, Verschleierung und Integration):

- **Platzierung (Vorbereitung auf das Geldspiel):** Spielbanken wandeln Bargeld (Fiatgeld) in Checks (Buchgeld) um, nehmen Umwandlungen von Stückelungen vor (smurfing). Auf Stufe der Spielenden kann der Umtausch in Fremdwährungen erfolgen. In den physischen Spielbanken wird mit Jetons gespielt, welche zuvor durch den Spieler direkt am Tisch oder an der Kasse oftmals gegen Bargeld umgetauscht wurden. Um die effektiven Eigentumsverhältnisse zu verbergen, können Strohmänner eingesetzt werden.
- **Herkunftsverschleierung (während des Geldspiels):** Vermehrt nehmen Kriminelle die Finanzdienstleistungen (beispielsweise Kundendepots oder internationalen Zahlungsverkehr) der Spielbanken in Anspruch. Die Kriminellen sind auch bereit, einen Teil ihrer Einsätze zu verlieren, um scheinbar legale Vermögenswerte zu erhalten.
- **Integrationsphase:** Um im grossen Stil Gelder über das Geldspiel waschen zu können, streben Kriminelle insbesondere im Ausland den Betrieb von Spielbanken an.[64]

[57] Homepage Spielbanken Sachsen, Beitrag vom 2. November 2022, Die Geschichte des Glücksspiels

[58] FATF Report, Vulnerabilities of Casinos and Gaming Sector, 2009, S.9.

[59] Bericht der Fachdirektorenkonferenz Geldspiele, Marktanteile des legalen und des illegalen Geldspielangebots in der Schweiz, Internet- und Sekundärdaten-Analyse, April 2024, S. 3.

[60] Studie des Schweizer Instituts für Sucht- und Gesundheitsforschung, Geldspiel: Verhalten und Problematik in der Schweiz 2022, Zusammenfassung, Zürich, Oktober 2024.

[61] Global Strategic Business Report, Mobile Gambling Market Assessment and Investment Opportunities, September 2024.

[62] The Department of the Treasury, 2024 National Money Laundering Risk Assessment (NMLRA), S. 81 ff.

[63] National Coordinating Committee on Combating Money Laundering and Funding of Terrorism, Malta's National Risk Assessment 2023, S. 115 ff.

[64] Erste nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei und Terrorismusfinanzierungsrisiken in der Schweiz, Juni 2015, S. 85.

Risiko- und Gesetzeslage in der Schweiz

Die Berichte über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz aus den Jahren 2015[65] und 2021[66] stufen das Risiko von Geldwäscherei in Bezug auf Spielbanken als sehr gering ein. Der Bericht aus dem Jahr 2021 führt ergänzend aus, dass das Risiko im Zusammenhang mit den erst 2019 eingeführten Schweizer Online-Spielbanken schwer zu bemessen ist.

Die strengen Voraussetzungen für die Vergabe einer Konzession, die in der Schweiz benötigt wird, um eine Spielbank (Casino) zu betreiben, könnte ein Grund für das geringe Risiko von Geldwäscherei sein. Per Ende 2024 hat der Bundesrat für die Jahre 2025 bis 2044 zehn Konzessionen ohne gesetzliche Beschränkung der Höchsteinsätze[67] und 12 mit Limitierung der Höchsteinsätze[68], also insgesamt 22 Konzessionen vergeben.[69] Die Vergabe der Konzessionen ist an strenge Prüfkriterien gebunden. Die Antragsteller sowie alle anderen involvierten Personen müssen einen guten Ruf geniessen[70] und eine einwandfreie Geschäftstätigkeit gewähren können. Die Antragsteller müssen zudem nachweisen können, dass sie über ein ausreichendes

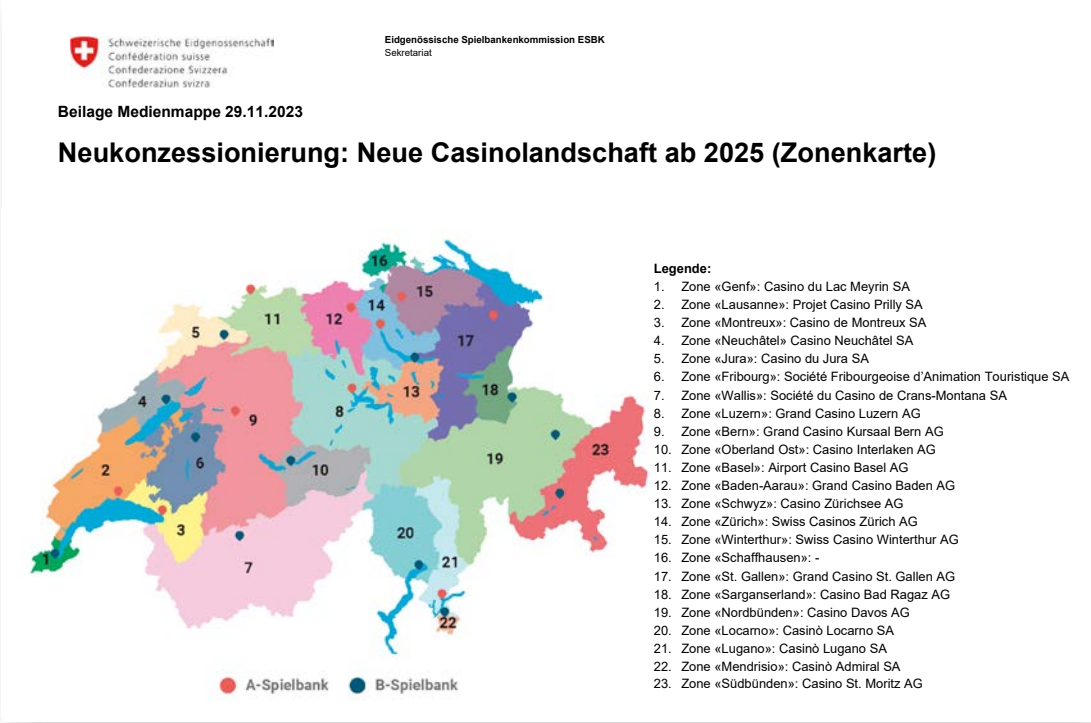


Abbildung 13: Eidgenössische Spielbankenkommission ESBK, Neukonzessionierung: Neue Casinolandschaft ab 2025 (Zonenkarte), November 2023.

65 Erste nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei und Terrorismusfinanzierungsrisiken in der Schweiz, Juni 2015, S. 5.

66 Zweite nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Oktober 2021, S. 45.

67 Konzession Typ A.

68 Konzession Typ B.

69 Medienmitteilung Bundesrat vom 29. November 2023: «Bundesrat vergibt Spielbankenkonzessionen: Kontinuität in der Casinolandschaft».

70 Botschaft zum Geldspielgesetz, BBl 2015 8387, 8441: Ein wichtiges Kriterium ist beispielsweise das frühere Verhalten auf dem Schweizer Markt. Es ist also davon auszugehen, dass z. B. jemand, der in der Vergangenheit ohne Bewilligung gezielt auf dem Schweizer Onlinespielbankenmarkt tätig war oder in der Schweiz oder im Ausland rechtskräftig verurteilt worden ist, das Kriterium des guten Rufs nach dem neuen Recht nicht erfüllen wird.

Sicherheitskonzept zur Bekämpfung von Kriminalität und Geldwäscherei verfügen.[71]

Das Geldspielgesetz gibt den bestehenden Spielbanken seit 1. Januar 2019 die Möglichkeit, ihre Spiele auch online anzubieten.[72] Sie benötigen dafür eine Konzessionserweiterung, die vom Bundesrat erteilt wird. Neben der Konzessionserweiterung bedürfen die Spielbanken zusätzlich der Bewilligung der Eidgenössischen Spielbankenkommission (ESBK) für die einzelnen Spiele, bevor sie ihre Online-Aktivität aufnehmen.[73] Die Spielbanken müssen sich im Sinne der Bekämpfung von Geldwäscherei an die GwG-Sorgfaltspflichten halten. Zehn Gesuchsteller haben für den neuen Zeitraum ab 2025 in der Schweiz eine solche Bewilligung erhalten.[74]

Der Fokus bei der Konzessionserteilung besteht darin, potentiell risikobehaftete Anbieter frühzeitig zu identifizieren und bereits vor der Erteilung der Konzession auszuschliessen. Auch während des Betriebs sind die Anbieter gehalten, die Vorgaben zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung einzuhalten.[75] So müssen die GwG-Sorgfaltspflichten bei der Eröffnung eines Spielerkontos für ein Online-Geldspiel eingehalten oder Abklärungen getätigt werden, wenn über das Spieler-Konto Transaktionen durchgeführt werden.[76] Während des Betriebs liegt der Fokus daher auf dem Spieler.

In der Schweiz sind ausschliesslich Anbieter zugelassen, die über eine Schweizer Konzession verfügen. Anbieter aus dem Ausland, die ihre Online-Spiele ohne Konzession in der Schweiz anbieten, sind verboten. Die ESKB sperrt diese Webseiten und veröffentlicht sie auf ihrer Sperrliste.[77]

Meldeverhalten in der Schweiz

Das Niveau der Verdachtsmeldungen, die von Schweizer Spielbanken stammen, ist seit über einem Jahrzehnt konstant tief. Zwischen 2014 und 2024 wurden durchschnittlich 0,5% der Verdachtsmeldungen von den Spielbanken (Casinos) abgesetzt. Im Jahr 2024 lag der Wert bei 0,3% (47 von 15 141 Verdachtsmeldungen; vgl. Tabelle 1).

Bei den 2024 eingegangenen Verdachtsmeldungen waren meist die Hintergrundabklärungen im Zusammenhang mit der Herkunft der Vermögenswerte, die zum Spielen verwendet wurden, ausschlaggebend. So kauften beispielsweise Spieler in physischen Casinos Jetons mit potentiell inkriminierten Geldern, spielten danach nur wenig und liessen sich die Jetons wieder auszahlen, bevor sie das Casino verliessen.

Weitere Verdachtsmeldungen hatten Abklärungen im Zusammenhang mit dem Spielerschutz als Ausgangslage. Die Spieler sollen zum Beispiel davor geschützt werden, die Kontrolle über ihr Geldspiel zu verlieren und von einem Weiterspiel abgehalten werden, um finanzielle Verluste zu verhindern. So sind die Spielbanken dazu verpflichtet, Spielsperren auszusprechen, wenn sie wissen oder annehmen, dass eine Person überschuldet ist oder wenn eine Person ihren finanziellen Verpflichtungen nicht mehr nachkommen kann.[78] Bei der Abklärung der Sperrvoraussetzungen kann beispielsweise festgestellt werden, dass der Spieler weder die Höhe der zum Spiel eingesetzten Mittel noch woher diese stammen plausibilisieren kann. Diese Umstände veranlassen die Spielbanken, weitere Abklärungen vorzunehmen und gegebenenfalls eine Meldung an die MROS zu erstatten.

Die Nutzung von Kryptowährungen ist in ausländischen Casinos eine relevante Thematik; in Schweizer Spielbanken ist sie bislang noch

71 Art. 8 Bundesgesetz über Geldspiele (Geldspielgesetz, BGS), SR 935.51.

72 Art. 9 BGS.

73 Eidgenössische Spielbankenkommission ESBK: Online-Spielbanken

74 Eidgenössische Spielbankenkommission ESBK: Online-Spielbanken

75 Art. 67 ff. BGS sowie Verordnung der Eidgenössischen Spielbankenkommission über die Sorgfaltspflichten der Spielbanken zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung ESBK, GwV-ESBK), SR 955.021.

76 Art. 52 i. V. m. Art. 47 Verordnung über Geldspiele (Geldspielverordnung, VGS), SR 935.511. Zu erwähnen sind auch die weiteren gesetzlichen Vorgaben zur Bekämpfung der Geldwäscherei, insbesondere, dass die Spielbanken keine Gewinnbestätigungen ausstellen dürfen (Art. 70 BGS) und es weitere Vorgaben bezüglich Checks und Depots gibt (Art. 69 BGS).

77 Eidgenössische Spielbankenkommission ESBK: Nicht bewilligte Online-Spiele

78 Bundesamt für Gesundheit (BAG), Geldspiel

nicht von Bedeutung. In der Schweiz sind Kryptowährungen als Zahlungsmittel derzeit verboten.[79]

Die Erkenntnisse aus der Strafverfolgung zeigen ein homogenes Bild zu den Meldezahlen: Es existieren lediglich wenige Urteile im Zusammenhang mit Geldwäscherei in Schweizer Casinos, die überwiegend kleinere Beträge betreffen. Der Inhaber eines Spielerkontos (X) wurde am 21. Juli 2023 gemäss Artikel 305bis Absatz 1 StGB per Strafbefehl durch die Staatsanwaltschaft Zug zu einer Geldstrafe verurteilt. Aus dem Urteil wird ersichtlich, dass das Benutzerkonto von X in dessen Wissen von anderen Personen benutzt wurde, um in einem Online-Casino zu spielen. Eine weitere Person (Y) nutzte die Gelegenheit und verwendete das Spielerkonto von X, um mit Geldern zu spielen, die sie sich zuvor illegal besorgt hatte. Y hatte sich die Bankdaten einer dritten Person (Z) verschafft, um sich anschliessend von deren Konto Gelder auf das Spielerkonto von X zu überweisen. Den Gewinn, den Y generiert hatte, liess sich X auf sein Konto überweisen, hob ihn in bar ab und überreichte ihn anschliessend Y.

Insgesamt lässt sich festhalten, dass Geldwäscherei im Zusammenhang mit Spielbanken in der Schweiz auf mehreren Ebenen bekämpft wird: Mit der Konzessionspflicht der Anbieter und den geldwäschereirechtlichen Massnahmen bei Spielerinnen und Spielern, welche im Vergleich zum Ausland streng sind. Zusätzlich werden nicht zugelassene Online-Spielbanken aus dem Ausland blockiert und auf einer Sperrliste publiziert. Dies impliziert, dass das Abwehrdispositiv der Schweiz greift und deswegen auch wenige Meldungen bei der MROS zu Online-Geldspielen eingehen.

4.2 Kinderpornografie und Virtual Assets

Die Polizeiliche Kriminalstatistik (PKS) erhebt jedes Jahr die Zahlen zu strafbarer Pornografie. Dieser Statistik ist nicht zu entnehmen, wie viele der Delikte explizit Kinderpornografie betrafen. Die Zahlen zu strafbarer Pornografie nach Artikel 197 StGB verzeichnen jedoch jedes Jahr bedauerliche Rekorde.[80] Auch wenn die Strafverfolgungsbehörden einige Erfolge gegen Pornografie-Ringe verzeichneten,[81] ist die Strafverfolgung in diesem Bereich schwierig.[82] Opfer und Täter befinden sich wegen der digitalen Vernetzung selten im gleichen Land. Dies wird auch in der Kriminalstatistik[83] deutlich, denn – selbst wenn der Missbrauch lokal erfolgt – die Bilder und Videos werden global verbreitet und konsumiert. 2023 wurden in der Schweiz 2967 Straftaten im Zusammenhang mit Pornografie verzeichnet,[84] 85,4% davon wurden online verübt.[85]

Kinderpornografie ist nach Artikel 197 StGB strafbar. Wenn der Tatbestand von Artikel 197 Absatz 4 StGB[86], erfüllt ist, drohen Freiheitsstrafen von bis zu fünf Jahren, womit es sich um ein Verbrechen handelt und eine Vortat zur Geldwäscherei darstellt.[87]

Angesichts der Tatsache, dass das Delikt Kinderpornografie überwiegend online begangen wird und für die betreffenden Inhalte regelmässig Zahlungen erfolgen, ist es umso erstaunlicher, dass die MROS im Jahr 2024 keine einzige Meldung erhielt, die den Verdacht auf Kinderpornografie anzeigte. Sie erhielt hingegen 70 Spontaninformationen von

[79] National Risk Assessment (NRA) – Bericht Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, Januar 2024, S. 39.

[80] Bundesamt für Statistik (BFS), Strafgesetzbuch (StGB): Straftaten und beschuldigte Personen, 2009 – 2023.

[81] SRF News: Ermittlungen in Deutschland – Grosse Kinderpornografie-Plattform abgeschaltet, Blick: Koordinierte Aktion im Tessin – Zwölf Menschen wegen illegaler Pornografie festgenommen

[82] Neue Zürcher Zeitung (NZZ): Kinderporno-Flut: Ermittler aus Zürich sagt, es werde immer schlimmer

[83] BFS, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten.

[84] BFS, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten, S.9.

[85] BFS, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten, S.62.

[86] Wer pornografische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen, die tatsächliche sexuelle Handlungen mit Minderjährigen zum Inhalt haben herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt, zugänglich macht, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt, kann gemäss Artikel 197 Absatz 4 StGB, zweiter Satz, mit einer Freiheitsstrafe von bis zu fünf Jahren oder einer Geldstrafe bestraft werden.

[87] Als Vortaten zur Geldwäscherei gelten Verbrechen, d. h. Taten, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind (vgl. Artikel 305bis Ziff. 1 i. V. m. Artikel 10 Abs. 2 StGB).

ausländischen FIUs. Diese Spontaninformationen führten in einigen Fällen zu Verknüpfungen mit Verdachtsmeldungen der MROS, bei denen die Finanzintermediäre die Vortat nicht eindeutig identifizieren konnten.

Die ausländischen FIUs teilten der MROS potenzielle Täter mit. Meist nutzten die Täter Krypto Wallets und andere, vermeintlich anonyme Zahlungsmethoden, um niedrige Beträge an Gegenparteien oder auf Konten und Wallets ins Ausland zu senden. Diese Feststellungen decken sich mit den Ergebnissen der Studie der internationalen Non-Profit-Organisation Internet Watch Foundation (IWF). Sie berichtet, dass für die Bezahlung von Kindsmissbrauchsmaterial (Child Sexual Abuse Material; CSAM) vorwiegend Kryptowährungen, Kreditkarten und Money-Transmitter eingesetzt werden.[88] Die meldenden Finanzintermediäre im Ausland konnten jeweils einen klaren Konnex der verwendeten Wallets, Konten oder potentiellen Tätern zum Delikt aufzeigen. Die Wohnadressen der Täter verteilen sich über die gesamte Schweiz; es gibt keinen geografischen Schwerpunkt. Die Opfer hingegen befinden sich vorwiegend in Asien, Osteuropa und Südamerika.

Schliesslich sind weder Kinderpornografie noch die virtuellen Zahlungsmöglichkeiten neue Phänome. Es besteht jedoch eine Diskrepanz zwischen den fehlenden Meldungen durch Schweizer Finanzintermediäre und den regelmässig eingehenden Spontaninformationen aus dem Ausland. Die MROS setzt sich daher für diese Lückenschliessung ein. Seit 2024 engagiert sie sich als Mitglied in der Arbeitsgruppe «Sexual Child Abuse» bei EFIPPP. Die gewonnen Erkenntnisse nutzt die MROS für die Sensibilisierung der Finanzintermediäre (beispielsweise FIAHT-Guide, vgl. dazu Kap. 2.5.1).[89]

Wann immer möglich sind die Finanzintermediäre gehalten, eine Verdachtsmeldung mit Angabe der vermuteten Vortat abzusetzen, sobald sie einen Indikator erkennen. Nur dann kann sichergestellt werden, dass die Meldung auch ohne zusätzliche Informationen aus dem Ausland bei der MROS korrekt und zielgerichtet analysiert und den Strafverfolgungsbehörden zugeführt werden kann.

4.3 Hamas-Verbot

Das GwG auferlegt den Finanzintermediären sowie den Händlerinnen und Händlern bereits heute Meldepflichten an die MROS in Bezug auf Terrorismusfinanzierung. Dies namentlich, wenn sie wissen oder der begründete Verdacht besteht, dass die in die Geschäftsbeziehung involvierten Vermögenswerte in Zusammenhang mit einer strafbaren Handlung nach Artikel 260ter StGB (kriminelle und terroristische Organisationen) stehen[90]; der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen[91] oder der Terrorismusfinanzierung dienen[92].

Eine der Herausforderungen für die Finanzintermediäre ist, die Terrorismusfinanzierung zu erkennen. Denn oftmals handelt es sich um «saubere», also nicht inkriminierte Gelder. Anders als bei einem Verdacht auf Geldwäscherei hat der Finanzintermediär somit nicht zu prüfen, ob die Vermögenswerte aus einer geldwäschereirelevanten Vortat stammen, sondern ob sie zukünftig zur Terrorismusfinanzierung dienen könnten. Dies ist offensichtlich schwierig zu erkennen; insbesondere in Konstellationen, in welchen Vermögenswerte zu Gunsten von Personen oder Organisationen ausgerichtet werden, die keine direkte Verbindung zu bekannten Terrororganisationen haben und deren Tätigkeiten bis anhin nicht als terroristisch eingestuft wurden. Die Erkennung und Bekämpfung von Terrorismusfinanzierung ex ante ist also schwieriger vorzunehmen, als – wie dies bei der Geldwäscherei der Fall ist – auf einen vergangenen Sachverhalt abzustellen. Hinzu kommt, dass es sich bei Beträgen zur Terrorismusfinanzierung oft um geringfügige Summen (Spenden zahlreicher Personen) handelt, bei welchen das (automatisierte)

88 Internet Watch Foundation, The Annual Report 2022, S. 85.

89 So z. B. auch in dem von der MROS herausgegebenen FIAHT-Guide für die Indikatoren zur Erkennung von Kinderpornografie: Financial Intelligence against Human Trafficking, Guide, S. 15 sowie S. 19 ff.

90 Vgl. Art. 9 Abs. 1 lit. a Ziff. 1 GwG.

91 Vgl. Art. 9 Abs. 1 lit. a Ziff. 3 GwG.

92 Vgl. Art. 9 Abs. 1 lit. a Ziff. 4 GwG.

Transaktionsmonitoring der Finanzintermediäre nicht anschlägt und deshalb keine vertieften Abklärungen veranlasst.[93]

Der Bundesrat hat am 4. September 2024 die Botschaft zum Bundesgesetz über das Verbot der Hamas sowie verwandter Organisationen an das Parlament verabschiedet.[94] Im Dezember 2024 beschloss die Bundesversammlung die Annahme des Bundesgesetzes.[95] Der Bundesrat bestimmt nach Ablauf der Referendumsfrist (19. April 2025) das Inkrafttreten. Ferner wurde der Bundesrat beauftragt, zusätzlich die Hisbollah zu verbieten. Das Verbot führt für die Finanzintermediäre zu mehr Rechtssicherheit, da sie nicht mehr selbst beurteilen müssen, ob es sich dabei um terroristische Organisationen handelt. Durch die Einstufung einer Gruppierung als terroristische Organisation wird auch für die MROS Klarheit geschaffen, indem eindeutig eine Vortat zur Geldwäscherei[96] stipuliert wird. Dies bildet die Grundlage für den Informationsaustausch mit ausländischen Partnerbehörden. Nehmen die Verdachtsmeldungen der Finanzintermediäre bezüglich Terrorismusfinanzierung zu, stehen auch mehr Informationen zur Verfügung, welche auf dem Weg der internationalen Amtshilfe mit dem Ausland geteilt werden können, was wiederum zur effektiveren Strafverfolgung beiträgt.

Seit dem Angriff vom 7. Oktober 2023 der Hamas auf Israel hat die MROS rund vierzig Verdachtsmeldungen im Zusammenhang mit der potenziellen Finanzierung der Hamas erhalten. Bei einer Vielzahl der Meldungen konnte die MROS Risiken im Zusammenhang mit Vereinen und Stiftungen ausmachen, die vorwiegend humanitäre Projekte unterstützen. Die öffentliche «Pro-Hamas»-Proklamation einiger Mitglieder solcher Institutionen veranlassten die MROS, die Finanzierung dieser juristischen Personen und die Geldflüsse eingehend zu analysieren. Eine vertiefte Analyse führte die MROS auch bei Verdachtsmeldungen zu Privatpersonen durch, die solche Erklärungen publik machten, Spenden erhalten sowie das Geld in bar abheben. Im Bereich der Kryptowährungen befassten sich einige in diesem Sektor tätige Finanzintermediäre mit der Analyse von Transaktionen mittels Blockchain. Häufig führten indirekte Verbindungen zu suspekt gekennzeichneten Wallets zu Verdachtsmeldungen.

Die MROS ist bestrebt, einen Überblick über mögliche Hamas-Finanzierungen aus der Schweiz zu erhalten. Fälle, in denen ein begründeter Verdacht auf Finanzierung einer terroristischen Organisation besteht, werden an die Bundesanwaltschaft übermittelt.

Zusammenfassend ergibt sich, dass das Inkrafttreten des Bundesgesetzes über das Verbot der Hamas sowie verwandter Organisationen Rechtssicherheit in Bezug auf die Qualifikation der Hamas als terroristische Vereinigung schafft. Die MROS analysiert die Entwicklung bei den eingehenden Meldungen mit Bezug zur Hamas laufend. Sie beobachtet, dass Vereinigungen und Stiftungen, welche humanitäre Projekte finanziell unterstützen, ein potentielles Risiko für Terrorismusfinanzierung aufweisen (vgl. Sensibilisierungsschreiben und Typologien an die Finanzintermediäre)[97].

[93] Zweite nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Oktober 2021, S. 48.

[94] Medienmitteilung Bundesrat vom 4. September 2024, «Der Bundesrat verabschiedet die Botschaft zum Verbot der Hamas».

[95] Schlussabstimmungstext vom 20. Dezember 2024, BBl 2025 21.

[96] Als Vortaten zur Geldwäscherei gelten Verbrechen, d. h. Taten, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind.

[97] Alert vom 3. November 2023 sowie Addendum vom 5. Dezember 2023. Dieser Alert setzte sich aus den Publikationen der FATF sowie Informationen ausländischer FIUs und Erkenntnisse der MROS zusammen; zu finden unter: Publikationen der Meldestelle für Geldwäscherei (MROS).

5 Aus der Praxis der Meldestelle

5.1 Unverzügliche Meldung vs. Abklärungstiefe – Standpunkt MROS

Die MROS stellte in den letzten beiden Jahren fest, dass es Defizite und qualitative Unterschiede hinsichtlich dem Inhalt der Verdachtsmeldungen gibt. Teilweise übermitteln die Finanzinstitute nur noch sehr rudimentär oder kaum abgeklärte Sachverhalte. Oder aber es ist für die MROS nicht erkennbar, ob besondere Abklärungen gemäss Artikel 6 GwG stattgefunden haben und damit eine konkrete Auseinandersetzung mit den Verdachtselementen erfolgte. Die MROS hat bereits im Jahresbericht 2023 auf diese Entwicklung hingewiesen und auf den allgemeinen Kostendruck zurückgeführt. Zudem machen die Finanzintermediäre geltend, dass der Druck, eine Meldung möglichst rasch abzusetzen, stark zugenommen habe. Sie sind der Meinung, dass die Behörden den Begriff «Unverzüglichkeit», der definiert wie schnell eine Meldung an die MROS abzusetzen ist, verschärft haben sollen. Ein drohendes Strafverfahren für die Finanzintermediäre und deren Mitarbeitende erhöht den Druck massiv.

Die MROS kann zu dieser Aussage nur soweit Stellung nehmen, soweit ihr Kernbereich, das operative Meldewesen, tangiert ist. Das schweizerische Geldwäschereiabwehrdispositiv fusst darauf, dass der Finanzintermediär die ersten grundlegenden Abklärungen hinsichtlich möglicher illegaler Vermögenswerte oder Transaktionen trifft. Der Gesetzgeber hat sich klar für ein qualitatives Meldewesen ausgesprochen. Auf sogenannte «schwellenwertbasierte» Meldungen, die beispielsweise eine bestimmte Transaktionssumme oder einen anderen quantitativen Trigger voraussetzen, wurde im Schweizer Recht bisher bewusst verzichtet. Die im Geldwäschereigesetz verankerten Sorgfaltspflichten sind kaskadenartig und repetitiv aufgebaut. Ausgangspunkt bilden die Artikel 3 – 5 GwG mit der Identifizierung der Vertragspartei, der Feststellung des wirtschaftlich Berechtigten sowie der periodischen Wiederholung dieser Pflichten. Die besonderen Abklärungspflichten in Artikel 6 GwG sehen vor, Hintergründe sowie den Zweck von Transaktionen und Geschäftsbeziehung risikobasiert zu prüfen. Die Finanzintermediäre sollen Hinweisen und Verdachtsmomenten nachgehen und diese sauber abklären. Erst wenn diese Abklärungen zu keinem Erfolg führen, bzw. Verdachtsmomente nicht ausgeräumt werden können und sich ein begründeter Verdacht manifestiert, ist eine Verdachtsmeldung an die MROS im Sinne von Artikel 9 GwG zu erstatten. Dieses skizzierte «Prüfprogramm» bedingt, dass die Finanzintermediäre die erforderliche Zeit aufwenden dürfen, um die nötigen Abklärungen in der gebotenen Tiefe zu tätigen. Der erforderliche Aufwand ist im Einzelfall, je nach Risiko, Sachlage und Komplexität der Geschäftsbeziehung, unterschiedlich. Der Finanzintermediär benötigt einen gewissen Spielraum bei der Wahl seiner Abklärungshandlungen und der Zeitspanne, die er dafür benötigt. Insofern lässt sich die korrekte, respektive angemessene Zeitdauer, welche Abklärungen in Anspruch nehmen dürfen, nicht schematisch festlegen – es ist immer der konkrete Einzelfall entscheidend. Ziel der Abklärungen muss jedoch sein, dass der Finanzintermediär der Sachlage auf den Grund gehen und sich eine fundierte Meinung bilden kann.

Verdachtsmeldungen und die ihr zugrunde liegenden Abklärungen müssen eine gewisse inhaltliche Qualität aufweisen, damit die MROS sie sinnvoll aufbereiten und verarbeiten kann. Rudimentär oder gar nicht abgeklärte Sachverhalte erschweren oder verunmöglichen eine Analyse. Solche Verdachtsmeldungen blockieren das Informationssystem und binden bei der MROS unnötig Ressourcen. Sie wirken sich nachteilig auf die Effizienz in der Meldungsbearbeitung aus und tragen damit gesamthaft zu einer Schwächung des Geldwäschereiabwehrdispositivs bei.

Spätestens seit der Einführung der risikobasierten Arbeitsweise der MROS bewegt sich die Meldestelle weg vom traditionellen Bearbeitungsansatz «Eine Meldung gleich eine Anzeige an die Strafverfolgungsbehörden», hin zu aktiver «Intelligence» und zur Vernetzung der ihr zur Verfügung stehenden Informationen. Nicht mehr die Verdachtsmeldung als solches, sondern deren Informationsgehalt steht im Mittelpunkt der Analyse.[98] Die Basis hierzu bilden inhaltlich fundierte und möglichst vollständig abgeklärte Sachverhalte. Diese Faktoren wirken sich hinsichtlich der Effektivität

[98] Vgl. Jahresbericht MROS 2023, Kap. 2.3.

stärker aus als der Zeitfaktor. Die Unverzüglichkeit darf nicht zulasten der Abklärungstiefe gehen.

Ebenso wichtig wie die ausreichende Abklärungstiefe ist auch die Vollständigkeit der Verdachtsmeldung. Die MROS erhält nach wie vor zahlreiche Meldungen mit ungenügenden oder unvollständigen Daten. Solche Meldungen muss die MROS zur Nachbesserung an die Finanzintermediäre zurückweisen, insofern diese nicht durch die MROS-Mitarbeitenden manuell korrigiert werden können. Dies bindet wiederum Ressourcen der MROS.[99] Konsequenz einer Rückweisung ist, dass die Meldung nicht bearbeitet werden kann. Eine Eingangsbestätigung nach Artikel 4 MGwV versendet die MROS den Finanzintermediären folgerichtig erst nach vollständigem und korrektem Eingang.

Sowohl die inhaltliche Tiefe der Abklärungen als auch die vollständige und strukturierte Dokumentation in der Verdachtsmeldungen an die MROS sind entscheidend für eine effektive Meldungsbearbeitung und die Unterstützung der Strafverfolgungsbehörden in der Bekämpfung der Geldwäscherei.

5.2 Auslegung von Artikel 11*a* GwG – Begründung von Auskunftsersuchen

Mit Artikel 11*a* GwG verfügt die MROS über die Möglichkeit, bei Finanzintermediären Informationen einzuholen, wenn sich aufgrund der Analyse der Meldungen nach Artikel 9 GwG bzw. Artikel 305ter Absatz 2 StGB oder von Informationen von ausländischen Meldestellen ergibt, dass die entsprechenden Finanzintermediäre mit Transaktionen oder Geschäftsbeziehungen am Sachverhalt beteiligt waren. Die Auskunftsersuchen der MROS an die Finanzintermediäre haben einerseits zum Ziel, erhaltene Verdachtsmeldungen in einen grösseren Zusammenhang zu stellen und andererseits, ausländische Meldestellen mit den zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung notwendigen Informationen zu versorgen (vgl. dazu Jahresbericht MROS 2023, Kap. 6.1). Diese Möglichkeit der Informationsbeschaffung stellt eines der wichtigsten Instrumente der MROS zur wirksamen Bekämpfung der Geldwäscherei und Terrorismusfinanzierung dar.

Mit der Zustellung von Verdachtsmeldungen nach Artikel 9 GwG bzw. Artikel 305ter Absatz 2 StGB oder von Informationen von ausländischen Meldestellen erhält die MROS zahlreiche – teilweise besonders schützenswerte – Personen- und Finanzdaten. Die MROS ist verpflichtet, die gesetzlichen Vorgaben zum Schutz der Daten einzuhalten. Dies betrifft insbesondere auch die Bekanntgabe von Informationen, welche beim Verfassen von Auskunftsersuchen an die Finanzintermediäre gestützt auf Artikel 11*a* GwG verwendet und offengelegt werden.

Der schweizerische Rechtsrahmen sieht grundsätzlich verschiedene gesetzliche Bestimmungen mit unterschiedlichen Ausprägungen vor, um den Schutz der Daten und spezifisch der Informationen von Verdachtsmeldungen zu gewährleisten. Übergeordnet steht mit Artikel 320 StGB die Verletzung des Amtsgeheimnisses. Weiter schreibt das GwG mit den Artikeln 9 und 10*a* GwG vor, dass Verdachtsmeldungen, die an die MROS übermittelt werden, streng vertraulich behandelt werden müssen respektive, dass Finanzintermediäre Informationen über verdächtige Transaktionen geheim zu halten haben, um mögliche Ermittlungen nicht zu gefährden.

Das GwG enthält keinen Rechtfertigungsgrund, um den Finanzintermediären eine Begründung für ein Ersuchen zukommen zu lassen. In der Konsequenz darf die MROS beispielsweise nicht offenlegen, aus welchem (Verdachts-)Grund eine Analyse läuft, noch in welchem Zusammenhang der Kunde mit einer solchen Verdachtsmeldung steht. Dadurch soll auch verhindert werden, dass die Finanzintermediäre eine Selektion der angefragten Informationen vornehmen, zumal sie verpflichtet sind, sämtliche von der MROS ersuchten Informationen herauszugeben (vgl. dazu Jahresbericht MROS 2023, Kap. 6.1).

[99] Vgl. Jahresbericht MROS 2023. Kap. 3.

Die MROS begründet deshalb ihre Auskunftsersuchen an die Finanzintermediäre praxisgemäss nicht. Angefragt und offengelegt werden einzig diejenigen Angaben zur Geschäftsbeziehung, die es dem Finanzintermediär ermöglichen, die Geschäftsbeziehung oder den Beziehungsinhaber zu identifizieren. Dazu gehört beispielsweise die Kontonummer, die IBAN oder der Name.

Weitere Begründungen, weshalb die Informationen angefragt werden und in welchem Zusammenhang diese stehen, sind den Auskunftsersuchen der MROS nicht zu entnehmen. Eine Begründung könnte dazu führen, dass die betroffenen Finanzintermediäre Kenntnis von den Zusammenhängen einer laufenden Analyse bei der MROS erhalten und dadurch eine Kollusions- oder Verdunkelungsgefahr geschaffen wird. Mit einem Auskunftsersuchen nach Artikel 11*a* Absätze 2 und 2bis GwG legt die MROS bereits implizit offen, dass sie Analysen betreffend die Kunden eines Finanzintermediärs tätigt. Die Finanzintermediäre können so annehmen, dass eine Verdachtsmeldung oder ein ausländisches Ersuchen zu dieser Person eingegangen ist. Darüber hinaus darf die MROS keine Informationen mit den Finanzintermediären teilen; sie könnten eine Amtsgeheimnisverletzung darstellen.

5.3 Meldepflicht vs. Melderecht

Das Schweizer Verdachtsmeldesystem kennt ein Nebeneinander von Melderecht nach Artikel 305ter Absatz 2 StGB und der Meldepflicht nach Artikel 9 GwG. Das Melderecht, welches seit dem 1. August 1994 in Kraft ist, wurde als gesetzlicher Rechtfertigungsgrund für die Finanzintermediäre geschaffen, damit sie sich nicht der Gefahr einer Verletzung des Berufsgeheimnisses aussetzen. Die Meldepflicht fand mit Einführung des GwG per 1. April 1998 eine rechtliche Grundlage.

Bereits mit Inkraftsetzung des Geldwäschereigesetzes stellte sich die Frage, ob es neben der Meldepflicht noch ein Melderecht braucht. Im Zuge der «SIF-Vorlage»[100] und der Einführung von Artikel 9 Absatz 1^{quater} GwG, mit welchem das Meldepflicht auslösende Element des begründeten Verdachts im Gesetz definiert und verankert wurde, stellte sich diese Frage erneut. Der Bundesrat schlug vor, das Melderecht zugunsten der Meldepflicht zu streichen. Er führte im erläuternden Bericht zur Vernehmlassungsvorlage[101] aus, dass es für das Melderecht nach Artikel 305ter Absatz 2 StGB kaum mehr ein Anwendungsbereich gibt. Der Sachverhalt, auf den das Melderecht abzielt, fällt mit Blick auf die Rechtsprechung schon weitestgehend unter die Meldepflicht von Artikel 9 GwG. Die Folgen einer Meldung nach Artikel 9 GwG und nach Artikel 305ter Absatz 2 StGB sind identisch: Die Vermögenswerte werden nicht automatisch gesperrt. Auch bei einer Weiterleitung der Anzeige durch die MROS an die Strafverfolgungsbehörden haben beide Meldungsarten die gleichen Konsequenzen: die Sperrung der anvertrauten Vermögenswerte während fünf Tagen.

In der Vernehmlassung zur «SIF-Vorlage» kritisierte die Branche die Aufhebung des Melderechts stark. Sie äusserte die Befürchtung, dass sich die Mitarbeitenden der Finanzintermediäre vermehrt dem Risiko einer Strafbarkeit wegen der Verletzung des Bankkundengeheimnisses aussetzen.[102] Dem ist entgegenzuhalten, dass nicht nur Artikel 305ter Absatz 2 StGB, sondern auch Artikel 11 GwG einen ausreichenden gesetzlichen Rechtfertigungsgrund enthält. Die Kritiken führten dazu, dass auf die Aufhebung des Melderechts verzichtet wurde. Die Botschaft führte dazu aus, dass das Melderecht subsidiär zur Meldepflicht ist. Der Finanzintermediär hat auch bei Wahrnehmung des Melderechtes die Pflicht, die Abklärungen zu den besonderen Sorgfaltspflichten nach Artikel 6 Absatz 2 GwG vorzunehmen. Das Melderecht kann nicht dazu benutzt werden, der MROS Fälle ohne vorherige Abklärungen zu melden. Der Bundesrat ging davon aus, dass mit dem neuen Wortlaut in Artikel 9 Absatz 1^{quater} GwG und der damit weiten Auslegung des begründeten Verdachts, die gestützt auf das Melderecht übermittelten Meldungen zugunsten

[100] AS 2021 656, siehe auch Botschaft vom 26. Juni 2019 zur Änderung des Geldwäschereigesetzes, BBl 2019 5451, 5477 ff.

[101] Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Erläuternder Bericht zur Vernehmlassungsvorlage.

[102] Siehe Ergebnisbericht zur Vernehmlassung zur Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Gelwäschereigesetz) vom 26. Juni 2019, Ziff. 8.1.1.

der auf die Meldepflicht gestützten Meldungen zurückgehen.[103]

Die Statistik (vgl. Kap. 3.4) verdeutlicht, dass die Meldungen, welche sich auf das Melderecht stützen, im Jahr 2023 signifikant zurückgingen. Auch im Jahr 2024 wurde ein leichter Rückgang verzeichnet. Die Frage stellt sich erneut: Ist ein Nebeneinander von Melderecht und Meldepflicht noch gerechtfertigt?

Die MROS macht in der Analyse keinen Unterschied zwischen Meldungen nach Melderecht und Meldepflicht. Zu beobachten ist aber, dass die Finanzintermediäre Meldungen nach Melderecht teilweise weniger tief abgeklärt und die übermittelten Informationen zu wenig Aussagekraft haben, um einen Verdacht zu erhärten. Die MROS erinnert daran, dass die Wahrnehmung eines Melderechts nicht von den Sorgfaltspflichten entbindet.

5.4 Definition des Begriffs Strafverfolgungsbehörden

Die MROS erstattet nach Artikel 23 Absatz 4 GwG Anzeige an die zuständigen Strafverfolgungsbehörden, wenn sie nach der Analyse einer oder mehrerer Verdachtsmeldungen einen begründeten Verdacht hat. Die MROS übermittelt die Anzeigen praxisgemäss an die kantonalen Staatsanwaltschaften und an die Bundesanwaltschaft. Weitere Behörden, welche als Strafverfolgungsbehörde qualifizieren, sind die Bundeskriminalpolizei, die kantonalen Polizeien oder Behörden, welche über einen Strafrechtsdienst verfügen und ebenfalls Vortaten im Sinne des Geldwäschereigesetzes bekämpfen. Der heutigen Praxis der MROS entsprechend werden diesen weiteren Strafverfolgungsbehörden Informationen aber nur als Spontaninformationen im Rahmen der Amtshilfe übermittelt. Es stellt sich daher die Frage, ob die MROS nebst Spontaninformationen in ausgewählten Fällen auch Anzeigen an diese weiteren Strafverfolgungsbehörden erstatten könnte.

Artikel 12 Strafprozessordnung (StPO)[104] listet neben der Staatsanwaltschaft auch die Polizei und die Übertretungsstrafbehörden als Strafverfolgungsbehörden auf. Während Letztere nicht in der Bekämpfung der Geldwäscherei oder deren Vortaten tätig sind, sieht dies bei der Polizei anders aus. Diese kann auch selbständig Ermittlungen an die Hand nehmen, sei dies aus eigenem Antrieb oder auf Anzeige hin (Art. 15 Abs. 2 StPO).

Die Organisation der Strafbehörden des Bundes ist im Strafbehördenorganisationsgesetz (StBOG)[105] geregelt. Gemäss Artikel 2 StBOG sind die Strafverfolgungsbehörden des Bundes die Polizei und die Bundesanwaltschaft. Als Polizeibehörden bezeichnet Artikel 4 StBOG (a) die Bundeskriminalpolizei, (b) andere Einheiten des Bundesamtes für Polizei, soweit das Bundesrecht vorsieht, dass sie Aufgaben im Rahmen der Strafverfolgung wahrnehmen, (c) andere Bundesbehörden, soweit das Bundesrecht vorsieht, dass sie Aufgaben im Rahmen der Strafverfolgung wahrnehmen sowie (d) kantonale Polizeikräfte, die im Zusammenwirken mit den Strafbehörden des Bundes Aufgaben im Rahmen der Strafverfolgung wahrnehmen. Gerade im Bereich des Verwaltungsstrafrechtes sind verschiedene Bundesämter für die Verfolgung von Straftaten (darunter auch Verbrechen, welche eine Vortat zur Geldwäscherei darstellen) zuständig.

Der Kreis der Behörden, an welche die MROS Anzeigen nach Artikel 23 GwG erstatten kann, ist somit weitaus grösser als die kantonalen Staatsanwaltschaften und die Bundesanwaltschaft. Die MROS behält sich darum vor, zukünftig auch Anzeigen an die Polizei oder Verwaltungsstrafbehörden zu erstatten. Die MROS wird die betroffenen Behörden jedoch vorgängig konsultieren. Die betroffene Behörde muss beachten, dass die Anzeigeerstattung eine Sperrung der Vermögenswerte zur Konsequenz hat. Falls die Behörde die Vermögenssperre aufrechterhalten will, muss sie innert fünf Arbeitstagen eine Verfügung erlassen (Art. 10 Abs. 2 GwG).

[103] Botschaft vom 26. Juni 2019 zur Änderung des Geldwäschereigesetzes, BBl 2019 5451, 5479.
[104] Schweizerische Strafprozessordnung (Strafprozessordnung, StPO), SR 312.0.
[105] Bundesgesetz über die Organisation der Strafbehörden des Bundes (StBOG), SR 173.71.

6 Internationale Zusammenarbeit in der Bekämpfung der Geldwäscherei

6.1 Egmont-Gruppe

Die Egmont-Gruppe[106], ein globales Netzwerk von FIUs, führte 2024 mehrere bedeutende Aktivitäten durch, um den internationalen Kampf gegen die Geldwäscherei und die Terrorismusfinanzierung zu stärken.

Ende Januar 2024 fanden die 24. jährlichen Arbeits- und Regionalgruppentreffen in St. Julian's, Malta, statt. Über 400 Vertreterinnen und Vertreter der FIUs sowie internationale Partner und Beobachter[107] nahmen daran teil. Die Treffen konzentrierten sich auf die Umsetzung der Strategie 2022 – 2027, die Identifikation von Unterstützungsmöglichkeiten im Bereich der Weiterbildung und der technischen Infrastruktur der FIUs. Weitere Schwerpunkte lagen bei den neuen Technologien, die von Kriminellen genutzt werden, und der Verbesserung des Informationsaustausches zwischen den FIUs.[108]

Die 30. jährliche Plenarsitzung der Egmont Gruppe fand vom 2. bis 7. Juni 2024 in Paris statt. Gastgeber war die französische FIU (Tracfin). Anwesend waren knapp 400 Vertreterinnen und Vertreter von FIUs sowie Beobachter. Hochrangige Redner, darunter der französische Wirtschaftsminister Bruno Le Maire und der damalige FATF Präsident T. Raja Kumar aus Singapur, eröffneten die Diskussionen. Die Plenary fokussierte sich insbesondere auf ein Thema: «The next generation FIU». Auf die FIUs kommen nicht nur technologische und personelle Herausforderungen zu (vgl. Kap. 2.4). Zudem stellt die Tatsache, dass kriminelle Netzwerke immer mehr und besser zusammenarbeiten, neue Technologien nutzen und ganz allgemein ressourcen- und IT-technisch besser ausgestattet sind als so manche FIU, das globale Netzwerk vor immer grössere Herausforderungen.[109]

Zur Stärkung der internationalen Zusammenarbeit bringt sich die MROS in den nächsten zwei Jahren noch intensiver in die Arbeit der Egmont-Gruppe ein. Die stellvertretende Leiterin der MROS und Leiterin des Bereiches Internationales wurde bei der Plenary in Paris für eine Amtszeit von zwei Jahren als Regionale Vertreterin von Europe II gewählt. Mitglieder dieser Region sind nebst der MROS unter anderem UK, Monaco, Guernsey, Jersey, Gibraltar, Isle of Man, Israel, Georgien und die Ukraine.

6.2 GAFI / FATF

6.2.1 Allgemein

Die Financial Action Task Force (FATF)[110] hat im Jahr 2024 mehrere, bedeutende Meilensteine erreicht, um die globale Bekämpfung von Geldwäscherei, Terrorismus- und Proliferationsfinanzierung zu stärken.

So veröffentlichte die FATF im März 2024 die risikobasierte Leitlinie zur Umsetzung der Empfehlung 25 (Transparency and Beneficial Ownership of legal Arrangements).[111] Juristische Personen, Trusts und weitere Rechtskonstrukte werden weltweit missbräuchlich eingesetzt, um Vermögenswerte zum Zwecke der Geldwäscherei, Terrorismusfinanzierung, Korruption oder Umgehung von Sanktionen zu verschleiern. Die Leitlinie hilft den Ländern und dem Privatsektor zu verstehen, wie Transparenzanforderungen auf rechtliche Vereinbarungen anzuwenden sind. Sie enthält praktische Hinweise zum Verständnis und zur Bewertung der mit Rechtskonstrukten und Trusts verbundenen Risiken. Sie dient, kriminelle Akteure, welche ihre kriminellen Aktivitäten mittels Briefkastenfirmen oder anderen komplexen Strukturen zu verstecken versuchen, besser zu identifizieren.

Die Schweiz ist sich der Risiken, welche mit der Verschleierung von kriminellen Vermögenswerten über rechtliche Strukturen verbunden sind, bewusst. Der Bundesrat hat daher im Mai 2024 eine Botschaft an das Parlament übermittelt. Ziel ist es, ein eidgenössisches Register (Transparenzregister) einzuführen, in welches Gesellschaften und andere juristische Personen ihre wirtschaftlich Berechtigten eintragen müssen. Dank dem Register werden ins-

[106] Vgl. Jahresbericht MROS 2023, Kap. 7.1.

[107] Beobachter sind keine FIUs. Es handelt sich dabei um Institutionen, welche dennoch die Möglichkeit erhalten, an den Egmont Group Meetings teilzunehmen. Als Beispiele zu nennen sind Europol, FATF oder die World Custom Organization.

[108] Egmont Group, 2024 Egmont Group Working and Regional Group Meetings (St. Julian's, Malta)

[109] Egmont Group, France's Financial Intelligence Unit (Tracfin) Hosts 400 EG Representatives from Around the Globe

[110] Zum Aufbau und den Aufgaben der Organisation vgl. Jahresbericht MROS 2023, Kap. 7.2.

[111] FATF, Guidance on Beneficial Ownership and Transparency of Legal Arrangements.

besondere die Strafverfolgungsbehörden schneller und zuverlässiger feststellen können, wer hinter einer Rechtsstruktur steht. Damit wird verhindert, dass juristische Personen und Trusts in der Schweiz zur Geldwäscherei oder zur Verschleierung von Vermögenswerten genutzt werden.[112]

Die FATF hat Algerien, Angola, die Elfenbeinküste und den Libanon 2024 in ihre sogenannte «graue Liste» aufgenommen. Senegal hat die FATF von der Liste gestrichen.[113] Die «graue Liste» wird drei Mal im Jahr von der FATF publiziert. Sie beinhaltet Länder und Gebiete, welche Schwachstellen in der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung aufweisen. Diese Länder arbeiten jedoch mit der FATF zusammen, um die strategischen Mängel in ihren Systemen zu beheben.[114]

Schliesslich ernannte die FATF Elisa de Anda Madrazo aus Mexiko für den Zeitraum vom 1. Juli 2024 bis zum 30. Juni 2026 zur neuen Präsidentin. Der Schwerpunkt der neuen Präsidentschaft liegt insbesondere auf der Umsetzung des risikobasierten Ansatzes, der Stärkung des globalen Netzwerkes, der Umsetzung der FATF-Standards und der finanziellen Inklusion.[115]

6.2.2 Länderevaluation

Im Oktober 2024 schloss die FATF die vierte Runde der gegenseitigen Länderevaluationen ab. Diese umfassende, «peer-to-peer» basierte Evaluation analysierte die Massnahmen von über 200 Mitgliedsländern im Hinblick auf die Bekämpfung von Finanzkriminalität, Terrorismusfinanzierung und Proliferation. Die Mutual Evaluation Reports (MER) analysieren den jeweiligen Fortschritt eines Landes, decken aber auch deren Schwachstellen auf. Die FATF zog eine Bilanz der 4. Evaluationsrunde und verabschiedete Anpassungen für die 5. Evaluationsrunde. Diese betreffen vor allem die Methodik und das Verfahren der gegenseitigen Evaluation.

Bei der nächsten Evaluationsrunde wird der Schwerpunkt noch stärker auf der Wirksamkeit der Abwehrdispositive liegen. Dies, um sicherzustellen, dass die Länder nicht nur über Gesetze, Vorschriften und Richtlinien verfügen, sondern diese auch effizient umsetzen und anwenden. Auch die Hauptrisiken der einzelnen Länder und der Kontext werden stärker in den Vordergrund gerückt. Dadurch stellt die FATF sicher, dass sich die Länder und die Prüfer auf die Bereiche konzentrieren, in denen die Risiken am höchsten sind. Für Bereiche mit geringerem Risiko ist es vergleichsweise einfacher, Ermittlungen einzuleiten und Verurteilungen zu erwirken. Die Empfehlungen aus den Berichten über die gegenseitige Evaluierung sind in Zukunft stärker ergebnisorientiert und konzentrieren sich auf spezifische Massnahmen und Zeitpläne zur Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und der Finanzierung von Massenvernichtungswaffen. Die nächste Evaluierungsrunde umfasst neu einen Sechsjahreszyklus, was deutlich kürzer ist und einen intensiveren Einsatz bedeutet.

Mit dem Start der 5. Evaluationsrunde begannen für die Schweiz und so auch für die MROS die Vorbereitungsarbeiten für die Evaluation der Schweiz. Der Lead für die Koordination liegt beim Staatssekretariat für Internationale Finanzfragen (SIF). Die Vorbereitungsarbeiten beschränken sich nicht nur auf die Behörden, sondern auch auf den Privatsektor und insbesondere die Finanzintermediäre. Diese nehmen einen wichtigen Teil in der Evaluation ein, da sie die «First Line of Defence» darstellen, wenn es um die Bekämpfung der Geldwäscherei und Terrorismusfinanzierung geht.

Die Schweiz wird in Zukunft auch Länderprüfer für die Evaluation anderer Länder stellen. Um die anspruchsvolle Aufgabe bestmöglich zu erfüllen, lässt die Schweiz Länderprüfer in sogenannten Joint Assessor Trainings (JAT) ausbilden. Die JAT finden mehrmals jährlich statt. Teilnehmen können Behördenvertreter der einzelnen Mitgliedsländer.

6.3 Taskforces

Die MROS bringt sich seit Jahren aktiv in mehreren, sowohl operativen als auch strategischen Task-

[112] Medienmitteilung Bundesrat vom 22. Mai 2024: «Bundesrat verabschiedet Botschaft zur Stärkung der Geldwäscherei-Bekämpfung».
[113] Publikation der FATF vom 25. Oktober 2024: «Outcomes FATF Plenary, 23 – 25 October 2024».
[114] Publikation der FATF, «Black and grey» lists
[115] Publikation der FATF, Objectives for the FATF during the Mexican Presidency (2024 – 2026).

forces ein. Anfang 2022 trat die MROS der Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS)[116] bei; Ende 2023 der Counter Terrorist Financing Taskforce Israel (CTFTI).[117] Über die Ziele und Tätigkeiten der Taskforces wurde bereits im Jahresbericht 2023 informiert. Im Jahr 2024 fanden mehrere Arbeitsgruppentreffen dieser Taskforces statt. Die MROS trat bei beiden Arbeitsgruppen je einmal als Gastgeberin auf.

6.4 Bilaterale Treffen

Die MROS engagiert sich für eine effiziente und reibungslose Zusammenarbeit mit den ausländischen Partner-FIUs. Die Kenntnis der bestehenden Grenzen sowie der rechtlichen Handlungsspielräume bei der Beschaffung relevanter Informationen von den jeweiligen Partnerbehörden ist nicht nur im Hinblick auf eine zügige Klärung der Sachverhalte von Bedeutung, sondern auch für einen ressourcenschonenden Einsatz der Mitarbeiterinnen und Mitarbeiter. Die bilateralen Treffen dienen dem strategischen Austausch zur Optimierung der Zusammenarbeit, insbesondere im Bereich der organisierten Kriminalität und der Terrorismusfinanzierung. Auch die technischen Möglichkeiten des Datenaustausches sowie die stetig wachsende Informationszufluss waren Themen, die sämtliche FIUs betreffen und daher eingehend diskutiert wurden.

2024 fanden mehrere bilaterale Treffen statt, unter anderem mit den FIUs aus Frankreich (Tracfin), USA (FinCEN), Italien (UIF), Moldawien, Montenegro, Österreich (A-FIU), Hong Kong (JFIU), Luxemburg (CRF) und Deutschland.

Ende September war die MROS Gastgeberin des dreitägigen Quad Island Forum-Treffens (neu: Quad Forum)[118]. Thematisiert wurden unter anderem die Wichtigkeit der Zusammenarbeit zwischen den Behörden und mit dem Privatsektor. Aufbauend auf dem Treffen zwischen der MROS und dem Quad Island Forum 2022 in London stellte die MROS das dort angekündigte und 2024 umgesetzte Swiss FIPPP vor. Zudem wurden auch die technischen Herausforderungen und die steigenden Datenmengen thematisiert. Es erfolgte ein wertvoller Austausch mit dem World Economic Forum[119] und der Wolfsberg Group[120]. Weitere Gastteilnehmende waren die FIU Luxemburg (CRF) und die FIU Monaco (AMSF).

Die Niederlande führte im Mai das deutschsprachige FIU-Treffen durch. Auch hier war eines der zentralen Themen der Umgang mit den exorbitant ansteigenden Datenmengen, die in Kontrast zu den überschaubar wachsenden personellen sowie technischen Möglichkeiten stehen. Weiter wurde die bevorstehende FATF-Länderevaluation diskutiert.

Die MROS unterzeichnete während der Egmont Plenarsitzung im Juli in Paris ein Memorandum of Understanding mit den FIU der Vereinigten Arabischen Emirate (UAE) und Kolumbien. Ziel ist es, die Zusammenarbeit weiter zu stärken.

[116] Financial Crimes Enforcement Network (FinCen), Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS Task Force).

[117] Financial Crimes Enforcement Network (FinCen), Counter Terrorist Financing Taskforce – Israel (CTFTI Task Force)

[118] Das «Quad Island Forum (neu: Quad Forum) of Financial Intelligence Units» ist ein strategischer Zusammenschluss der FIUs Gibraltar, Guernsey, Isle of Man und Jersey.

[119] Homepage The World Economic Forum.

[120] Homepage The Wolfsberg Group.

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.

Die MROS ist in sechs Bereiche gegliedert, die jeweils spezifische Aufgaben vorsehen. Im Jahr 2024 beschäftigte die MROS durchschnittlich 60 Mitarbeitende (51 Vollzeiteinheiten).

Das Organigramm stellt die aktuelle Organisation der MROS dar.

Planung und Policy (PuP)

Der Bereich PuP fungiert als klassische Querschnittsdisziplin und befasst sich mit vielschichtigen Themenbereichen. PuP bearbeitet sämtliche juristischen Fragestellungen sowie politische Dossiers bis auf Stufe Bundesrat (z. B. Gesetzesvorlagen, Motionen, Postulate, etc.). Zusätzlich begleitet und bearbeitet der Bereich Projekte und Publikationen (u. a. Jahresberichte, NRA, Typologien), kümmert sich um das Risikomanagement und dient als Ansprechpartner für sämtliche internen und externen Anfragen auf formeller und materieller Ebene. PuP unterstützt die operativen Bereiche der MROS und sichert die Unité de doctrine. Der Bereich pflegt den regelmässigen Austausch mit anderen Behörden und kümmert sich um die administrativen Belange der MROS.

Primäranalyse (PA)

Der Bereich PA ist für die Erfassung und Aufbereitung aller eingehenden Meldungen in formeller, technischer und inhaltlicher Hinsicht verantwortlich. Dies beinhaltet ebenfalls manuelle Korrekturen bei mangelhafter Datenqualität. Darüber hinaus übernimmt er die Triage, übergibt die Fälle anhand einer Gesamtbewertung an einen der nachgelagerten Bereiche oder bearbeitet und leitet Meldungen direkt an Strafverfolgungsbehörden weiter. Ebenfalls in die Zuständigkeit fällt die nationale Amtshilfe nach Artikel 29 GwG.

Operative Analyse Kantone (OAK)

Der Bereich OAK analysiert eingehende Verdachtsmeldungen, welche mehrheitlich in die Zuständigkeit der kantonalen Strafverfolgungsbehörden fallen und vom Bereich PA zugewiesen wurden. Bei begründetem Verdacht werden die aggregierten Informationen an die jeweils zuständige Strafverfolgungsbehörde übermittelt (in der Regel kantonale Strafverfolgungsbehörden). Informationen können im Zuge eines Informationsaustausches mit anderen nationalen Behörden sowie FIUs anderer Länder geteilt werden. Die Fälle betreffen unter anderem die strafbaren Handlungen gegen das Ver-

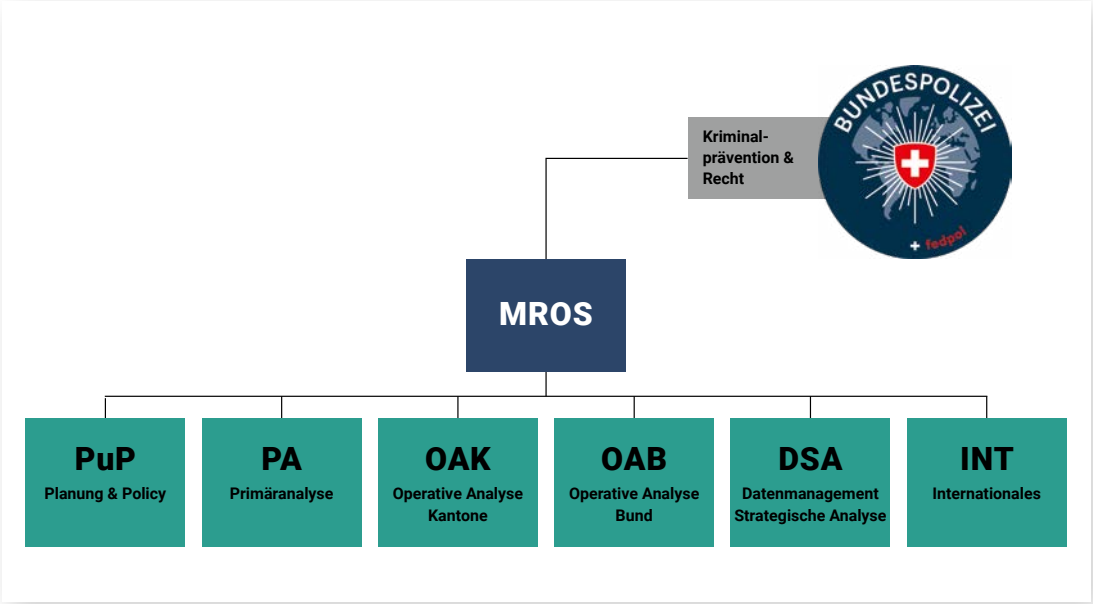


Abbildung 14: Organigramm MROS

mögen (hauptsächlich Betrug, Veruntreuung und ungetreue Geschäftsbesorgung), Menschenhandel und Urkundenfälschung.

Operative Analyse Bund (OAB)

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

Datenmanagement und strategische Analyse (DSA)

Der Bereich DSA verantwortet die Sicherheit des Betriebs des Informationssystems goAML und seine fachliche Entwicklung. Er bietet den Finanzintermediären technischen Support, insbesondere bei der Programmierung ihrer 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 kümmert sich um den gesamten (Informations-)Austausch mit ausländischen FIUs sowie um die Mitgliedschaft und Teilnahme an internationalen Gremien (u. a. Egmont Group, FATF, United Nations Convention against Corruption (UNCAC) und Europol Financial Intelligence Public Private Partnership (EFIPPP)).