ONLINEKOMMENTAR
DER FREI ZUGÄNGLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 23 GwG

Eine Kommentierung von Anton Brönnimann
Herausgegeben von Damian K. Graf / Doris Hutzler

Stand der Bearbeitung: 11.02.2025
PDF erstellt am: 06.10.2026
DOI: 10.17176/20250204-215311-0

ZITIERVORSCHLAG

Anton Brönnimann, Kommentierung zu Art. 23 GwG in: Damian K. Graf/Doris Hutzler (Hrsg.), Onlinekommentar zum Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung

Kurzzitat: OK-Brönnimann, Art. 23 GwG N. XXX.

4. Abschnitt: Meldestelle für Geldwäscherei

Art. 23

[1] Das Bundesamt für Polizei führt die Meldestelle für Geldwäscherei.

[2] Die Meldestelle prüft und analysiert die eingegangenen Meldungen. Soweit nötig holt sie nach Artikel 11*a* zusätzliche Informationen ein.

[3] Sie unterhält ein eigenes Informationssystem zur Bekämpfung der Geldwäscherei, von deren Vortaten, der organisierten Kriminalität und der Terrorismusfinanzierung.

[4] Sie erstattet der zuständigen Strafverfolgungsbehörde unverzüglich Anzeige, wenn sie begründeten Verdacht schöpft, dass:

a. eine strafbare Handlung nach Artikel 260ter, 305bis oder 305ter Absatz 1 StGB vorliegt;

b. Vermögenswerte aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Artikel 305bis Ziffer 1bis StGB herrühren;

c. Vermögenswerte der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen; oder

d. Vermögenswerte der Terrorismusfinanzierung (Art. 260^{quinquies} Abs. 1 StGB) dienen.

[5] Übermittelt sie die von einem Finanzintermediär nach Artikel 9 Absatz 1 Buchstabe a dieses Gesetzes oder nach Artikel 305ter Absatz 2 StGB gemeldeten Informationen einer

Strafverfolgungsbehörde, so informiert sie den Finanzintermediär darüber, solange dieser die Geschäftsbeziehung nicht nach Artikel 9*b* abgebrochen hat.

6 ...

GLIEDERUNG

I. Einleitung 4
II. Einfluss durch internationale Vorgaben 5
A. Allgemeines 5
B. FATF-Empfehlung 29 – Financial Intelligence Unit 5
C. Mitgliedschaft in der Egmont Gruppe und Einhaltung der Egmont Prinzipien 6
D. Verhältnis von Soft Law zum nationalen Recht 7
III. Regelungsinhalt 8
A. Organisation – Die Meldestelle als Teil der fedpol (Abs. 1) 8
1. Eingliederung der Meldestelle in fedpol 8
2. Umsetzung der internationalen Vorgaben ins nationale Recht 10
B. Die Analyse von Verdachtsmeldungen – «Intelligence» (Abs. 2) 11
1. Grundsatz 11
2. Instrumente der Analyse – «Toolbox» der Meldestelle 12
a. Informationen der Finanzintermediäre 13
b. Zugriff auf Polizei- und Justizdatenbanken 14
c. Informationen aus der internationalen Amtshilfe 14
d. Informationen aus der nationalen Amtshilfe 15
e. OSINT und weitere Informationsquellen 15
3. Risikobasierter Ansatz 15
C. Informationssystem (Abs. 3) 16
1. Einsatz der Softwareapplikation «goAML» 16
2. Bearbeitungsgrundsätze 17
D. Anzeige an die Strafverfolgungsbehörden (Abs. 4) 17
E. Mitteilung an den Finanzintermediär (Abs. 5) 19
Literaturverzeichnis 20
Materialienverzeichnis 21

I. EINLEITUNG

1 Die Meldestelle für Geldwäscherei MROS[1] (nachfolgend: «Meldestelle» oder «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.[2] FIU ist die international gebräuchliche Bezeichnung für staatliche Dienststellen, die bei der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung für Finanztransaktionsuntersuchungen zuständig sind. Der Meldestelle kommt eine wesentliche Funktion in der Kriminalitätsbekämpfung zu – sie spürt inkriminierte Vermögenswerte auf und folgt dem Grundsatz: «follow the money». Somit trägt sie massgeblich zur Glaubwürdigkeit des Schweizerischen Geldwäschereiabwehrdispositivs bei und schützt damit auch die Reputation des Schweizer Finanzplatzes.[3]

2 Die **Aufgaben und Kompetenzen** der Meldestelle leiten sich aus dem Geldwäschereigesetz (GwG), der Verordnung über die Meldestelle für Geldwäscherei (MGwV), der Geschäftsordnung fedpol/MROS sowie den internationalen Empfehlungen der Financial Action Task Force (FATF)[4] und den Verpflichtungen gegenüber der Egmont Gruppe[5] ab. Zu den Kernaufgaben der MROS zählen demnach: (1) **«Intelligence»**: Die Meldestelle empfängt Verdachtsmeldungen, welche gestützt auf das Geldwäschereigesetz und das Strafgesetzbuch von Finanzintermediären und den weiteren GwG-Unterstellten erstattet werden. Sie reichert diese mit zusätzlichen Informationen an und führt eigene Analysen durch. Sie entscheidet daraufhin im Einzelfall, ob die gewonnenen Informationen in Form einer Anzeige an eine Strafverfolgungsbehörde übermittelt werden oder nicht. (2) **«Kooperation»:** Die Meldestelle tauscht sich mit anderen nationalen Behörden sowie mit ausländischen FIUs auf dem Weg der Amtshilfe in operativen und strategischen Belangen aus. (3) **«Prävention»**: Die Meldestelle trägt zur Bewertung der nationalen Risiken von Geldwäscherei und Terrorismusfinanzierung bei. Sie betreibt strategische Analyse (Erkennen von Mustern und Tendenzen) und teilt die gewonnenen Erkenntnisse mit Behörden, der Finanzindustrie sowie der Öffentlichkeit.

3 Art. 23 GwG bildet die **gesetzliche Grundlage** der Meldestelle. Dieser äussert sich im Grundsatz zur Organisation, zur Analyse der Verdachtsmeldungen sowie zu den Voraussetzungen der Anzeige und der Weitergabe von Informationen an die Strafverfolgungsbehörden. Art. 23 darf jedoch nicht isoliert betrachtet werden – er steht im engen Kontext zu Art. 9, 11a, 29–32, 35 und 35a GwG sowie den internationalen Empfehlungen der FATF und den Prinzipien der Egmont Gruppe. Art. 23 GwG ist in den vergangenen 25 Jahren zumindest im Kern nicht revidiert worden – teilweise haben die internationalen aber auch die technischen Entwicklungen seinen Wortlaut überholt.[6] Der gelebten Praxis durch die Meldestelle und der geltungszeitlichen Auslegung von Art. 23 GwG kommen damit eine zentrale Bedeutung zu.

1. MROS ist die Abkürzung für Money Laundering Reporting Office Switzerland. International ist heute jedoch die Bezeichnung Financial Intelligence Unit (FIU) Switzerland vorherrschend.
2. OFK-Thelesklaf, Art. 23 GwG N. 1.
3. Vgl. Strategie MROS 2024–2027.
4. https://www.fatf-gafi.org/en/home.html, besucht am 30.11.2024.
5. https://egmontgroup.org/, besucht am 30.11.2024.
6. Vgl. Ursprungstext von Art. 23 GwG: Botschaft GwG 1996, S. 1172; Revidierte Texte von Art. 23 GwG: BBI 2007, S. 6315; BBl 2012, S. 6990; BBl 2014, S. 719; BBl 2018, S. 6538; BBl 2019, S. 5563.

II. EINFLUSS DURCH INTERNATIONALE VORGABEN

A. Allgemeines

4 Das nationale Geldwäschereiabwehrdispositiv wird nachhaltig durch **internationale Standards** beeinflusst. Die Schweiz ist Mitglied der im Jahr 1989 gegründeten Financial Action Task Force (FATF). Die FATF ist das wichtigste internationale Gremium zur Bekämpfung und Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung. Für diesen Bereich setzt sie Standards – in insgesamt 40 Empfehlungen wurden einheitliche Verhaltensregeln und Massstäbe definiert, die für den gesamten Finanzsektor sowie für alle beteiligten Personen und Berufsgruppen gelten.[7] Die FATF verabschiedet regelmässig verschiedene Auslegungsgrundsätze, insbesondere «Guidance»- und «Best-Practice»-Papiere. Die FATF fördert die weltweite Verbreitung dieser Standards und überprüft deren Umsetzung in ihren Mitgliedstaaten.[8]

5 Die Weltbank, der Internationale Währungsfonds und der Sicherheitsrat der UNO haben die FATF-Empfehlungen als internationale Standards anerkannt, obwohl sie kein unmittelbar bindendes Recht darstellen und ihnen damit lediglich der Status von Soft Law zukommt.[9] Weltweit haben sich über 180 Länder verpflichtet, die FATF-Empfehlungen zu übernehmen.

6 Um den Veränderungen im Standard gerecht zu werden, wurde das GwG in den vergangenen 25 Jahren mehrfach und grundlegend angepasst. Auch die MROS war von solchen **Änderungen** massgeblich betroffen, zumal sich diverse Empfehlungen, schwerpunktmässig die Empfehlung 29, aber auch die Empfehlungen 1 (Risikobewertung), 2 (nationale Zusammenarbeit und Koordination), 20 und 23 (Verdachtsmeldungen), 31 (Strafverfolgungs- und Ermittlungsbehörden), 33 (Führen von Statistiken) und 40 (internationale Zusammenarbeit) mit der Rolle und der Tätigkeiten der FIU befassen oder auf diese direkt oder indirekt Bezug nehmen.

B. FATF-Empfehlung 29 – Financial Intelligence Unit

7 Die FATF-Empfehlung 29 befasst sich ausschliesslich mit der **Funktion der FIU** und äussert sich in der Interpretativnote zur Organisation und zum Umfang der Aufgaben und ihrer Erfüllung. Der FATF-Standard verlangt, dass jedes Land über eine zentrale Meldestelle für Verdachtsmeldungen – eine Financial Intelligence Unit (FIU) – verfügt. Letztere ist auf nationaler Ebene für den Empfang und die Analyse von Verdachtsmeldungen bezüglich Geldwäscherei, deren Vortaten und Terrorismusfinanzierung zuständig. Sie leitet ihre Erkenntnisse aus der Analyse spontan oder auf Anfrage an die zuständigen Behörden weiter.[10]

8 Zur **Erfüllung ihrer Aufgaben** muss eine FIU in der Lage sein, zusätzliche Informationen von den Meldepflichtigen einzuholen. Sie sollte zudem über einen möglichst unmittelbaren und umfassenden Zugriff zu relevanten Behördeninformationen (Staatsanwaltschaft, Polizei, Aufsicht, weitere Verwaltungsbehörden etc.) verfügen, sowie Zugang zu öffentlichen Quellen und gegebenenfalls zu kommerziell angebotenen Datenbanken haben.[11]

9 Eine FIU muss zudem operativ **autonom** sein, d.h. sie muss in ihren Kerntätigkeiten – Entgegennahme von Meldungen, Priorisierung und Triage, Informationsbeschaffung, Art und Weise der Analyse und Analysemethoden, Datenmanagement, Weiterleitung und Austausch von

7. Vgl. FATF-Empfehlungen.
8. https://www.fatf-gafi.org/en/the-fatf/what-we-do.html, besucht am 30.11.2024.
9. Botschaft GwG 2014, S. 650 f.; Taube, S. 211.
10. FATF-Empfehlungen, S. 24 und S. 106 ff.
11. Interpretativnote zur FATF-Empfehlung 29 (C. [N. 5 f.]).

Informationen sowie Zusammenarbeit mit anderen Behörden unabhängig und weisungsungebunden agieren können. Als wesentliches Merkmal der Autonomie gilt, dass die FIU mit angemessenen finanziellen, personellen und technischen Ressourcen ausgestattet wird, damit sie ihre Aufgaben erfüllen kann. Operative Unabhängigkeit bedeutet nicht, dass eine FIU zwingend eine eigenständige Behörde sein muss. Sie kann Teil einer bereits bestehenden Behörde sein – diesfalls ist aber sicherzustellen, dass die Kernaufgaben der FIU von denjenigen der anderen Behörde getrennt sind.[12] Gleiches gilt auch bezüglich des Umgangs mit Daten. Die FIU hat dafür zu sorgen, dass die Sicherheit der empfangenen Daten gewährleistet ist und nur Mitarbeitende der FIU auf die entsprechenden Datenverarbeitungssysteme und IT-Applikationen zugreifen können.[13]

10 Abschliessend verlangt die FATF-Empfehlung 29 auch, dass die FIU die Grundsätze der Egmont Gruppe im internationalen Informationsaustausch anwendet. De facto verlangt der FATF-Standard von der FIU damit eine **dauerhafte Mitgliedschaft** bei der Egmont Gruppe.[14]

C. Mitgliedschaft in der Egmont Gruppe und Einhaltung der Egmont Prinzipien

11 Die Meldestelle ist seit 1998 Mitglied der 1995 gegründeten Egmont Gruppe[15], welche derzeit weltweit 177 FIU vereint.[16] Diese Organisation ermöglicht einen internationalen, gesicherten, raschen und rechtlich zulässigen **Austausch von Informationen** zur Bekämpfung von Geldwäscherei. Die Mitgliedschaft in der Egmont Gruppe ist für einen Finanzplatz der Grösse und Bedeutung der Schweiz zentral und alternativlos. Die Aufnahme und der Verbleib sind an strenge Qualifikationsmerkmale gebunden. Die Mitgliedschaft verleiht einer FIU eine Art Qualitätsgütesiegel und ist Garant für einen sicheren und standardisierten Informationsaustausch auf internationaler Ebene.[17] Die Mitgliedschaft ist inzwischen auch Teil der FATF-Standards.[18] Gewisse FIU sind zudem nur bereit, Informationen via das «Egmont Secure Web» – ein gesichertes elektronisches Informationssystem – auszutauschen, was die Mitgliedschaft bei der Egmont Gruppe voraussetzt.

12 Zur **operativen Unabhängigkeit** hat die Egmont Gruppe 2018 eine Publikation veröffentlicht: *«Understanding FIU Operational Independence and Autonomy»*. In Kapitel 6 werden die Charakteristika einer unabhängigen FIU beschrieben. Im Kern gehen die Anforderungen der Egmont Gruppe punkto der operativen Autonomie weiter als die FATF-Empfehlung 29. Namentlich verlangt der Egmont-Standard die räumliche Trennung der FIU von anderen staatlichen Behörden.[19] Auch die Bestellung von Personal, die Budgetkompetenz und die Möglichkeit, Dienstreisen zu unternehmen, sind restriktiver geregelt und sollen auf Stufe FIU abschliessend entschieden werden.[20] Ebenfalls unterliegt die Berufung und Abberufung des Leiters der FIU besonderen Kriterien, die nicht zwingend mit den personalrechtlichen Vorgaben der jeweiligen Jurisdiktion korrespondieren.[21] Zur Selbstbeurteilung der operativen Unabhängigkeit und Autonomie stellt die Egmont Gruppe eine Checkliste mit den relevanten Kriterien zur Verfügung.[22]

13 FIUs, die den sich stetig weiterentwickelnden Grundsätzen der Egmont Gruppe nicht mehr genügend nachkommen und/oder gegen diese verstossen, werden wegen Nichteinhaltung der Prinzipien einem

12. Interpretativnote zur FATF-Empfehlung 29 (E. [N. 8 ff.] und F. [N. 12]).
13. Interpretativnote zur FATF-Empfehlung 29 (D. [N. 7]).
14. Interpretativnote zur FATF-Empfehlung 29 (G. [N. 13]).
15. https://egmontgroup.org/members-by-region/eg-member-fiu-information/, besucht am 30.11.2024.
16. Stand der Mitgliedschaft per 30.11.2024.
17. Botschaft GwG 2012, S. 6950.
18. Interpretativnote zur FATF-Empfehlung 29 (G. [N. 13]).
19. Understanding FIU Operational Independence and Autonomy, N. 53.
20. Understanding FIU Operational Independence and Autonomy, N. 55 ff.
21. Understanding FIU Operational Independence and Autonomy, N. 59 ff.

sogenannten **Non-Compliance Verfahren** unterworfen, welches bei Nichtbehebung der festgestellten Defizite Verwarnungen, Suspendierungen und als Ultima Ratio den Ausschluss aus der Egmont Gruppe vorsieht.[23]

D. Verhältnis von Soft Law zum nationalen Recht

14 Soft Law zeichnet sich dadurch aus, dass es nicht einer der in Art. 38 IGH-Statut[24] genannten formellen Völkerrechtsquellen entstammt und somit nicht rechtsverbindlich ist. Vielmehr ist es **rechtsstützend oder rechtsergänzend**. Die Unverbindlichkeit des Soft Law hat zur Folge, dass seine Missachtung keine völkerrechtliche Verantwortung des betreffenden Staates auslöst und Repressalien völkerrechtlich unzulässig sind. Indessen bleiben Retorsionen oder Listings erlaubt. Erscheinungsformen von Soft Law können z.B. Resolutionen, Deklarationen, Empfehlungen, und Verhaltenskodizes internationaler Organisationen, Standards, best practice, principles sowie rechtlich nicht bindende Vereinbarungen (z.B. Memorandum of Understanding) sein. Ein wesentliches Indiz für das Vorliegen von Soft Law ist die Existenz eines Überwachungsverfahrens (sog. follow-up procedures) über die Einhaltung der im betroffenen Regelwerk enthaltenen Vorgaben.[25]

15 Die FATF ist keine internationale Organisation im Sinne des Völkerrechts, sondern ein rein politisches Gremium, weshalb ihre Empfehlungen und Publikationen keine unmittelbar bindende Wirkung für die beteiligten Staaten haben und damit lediglich «soft law» darstellen. Die FATF und ihre Mitgliedstaaten haben jedoch den klaren Anspruch, dass ihre Empfehlungen befolgt werden. Mittels jährlich durchzuführender Selbstbewertungen der Mitgliedsländer sowie Länderexamen, welche durch Evaluatoren anderer Mitgliedstaaten periodisch durchgeführt werden (sog. «mutual evaluations»), stellt die FATF sicher, dass ihre Empfehlungen ernst genommen und eingehalten werden.[26] Dreimal pro Jahr veröffentlicht die **FATF Listen** mit Ländern, welche strategische Defizite bei der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung aufweisen bzw. die Empfehlungen nicht einhalten:[27] Auf der sog. «schwarzen Liste»[28] landen alle jene Jurisdiktionen, welche ein Risiko für das internationale Finanzsystem darstellen und zudem die internationalen Bemühungen im Kampf gegen die Geldwäscherei und die Terrorismusfinanzierung erschweren oder gar verhindern. Indessen reihen sich auf der sog. «grauen Liste»[29] alle jene Jurisdiktionen ein, die keine ausreichenden Fortschritte bei der Behebung der Defizite gemacht oder sich nicht zu einem gemeinsam mit der FATF entwickelten Massnahmenplan verpflichtet haben.

16 Die Aufführung auf der schwarzen Liste hat keine direkten Konsequenzen für das jeweils aufgeführte Land – die FATF kann keine unmittelbar harten Massnahmen verfügen. Sie fordert ihre Mitgliedstaaten sowie auch andere Jurisdiktionen jedoch dazu auf, **Gegenmassnahmen** gegen diese Länder einzuleiten, um das internationale Finanzsystem vor Risiken der Geldwäscherei oder Terrorismusfinanzierung zu bewahren. Betreffend die Länder, welche auf der grauen Liste aufgeführt sind, ruft die FATF ihre Mitgliedstaaten dazu auf, die Risiken zu berücksichtigen, welche von den identifizierten Defiziten ausgehen.[30] Diese Aufforderungen sind in der FATF-Empfehlung 19

22. Understanding FIU Operational Independence and Autonomy, Annex C.
23. Egmont Charter, Ziff. 8 i.v.m. Egmont Compliance Process, S. 18; vgl. auch Botschaft GwG 2012, S. 6949.
24. Statut des Internationalen Gerichtshofs vom 26.6.1945 (SR 0.193.501).
25. Naef, S. 1110; Thürer, 433 f.
26. KV-KO-Ackermann/Zehnder, Art. 305bis StGB N. 49; Thürer, 433 ff.; Taube, 211; Naef, S. 1109 ff.
27. https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html, besucht am 30.11.2024.
28. Per 30.11.2024 befinden sich Nordkorea, Iran und Myanmar auf der schwarzen Liste.
29. Per 30.11.2024 befinden sich Algerien, Angola, Bulgarien, Burkina Faso, Elfenbeinküste, Kamerun, Kroatien, Demokratische Republik Kongo, Haiti, Kenia, Libanon, Mali, Monaco, Mosambik, Namibia, Nigeria, Philippinen, Südafrika, Südsudan, Syrien, Tansania, Venezuela, Vietnam und Jemen auf der grauen Liste.
30. Taube, S. 210 ff., m.w.H.

verankert, somit gleichermassen Teil des FATF-Standards und damit von der regelmässigen Prüfung durch die FATF erfasst. Mittels einer eigenständigen Empfehlung verfügt die FATF damit über ein starkes Druckmittel, um die Mitgliedsländer zu einem konformen Verhalten zu zwingen.[31]

17 Das «Sanktionssystem» der FATF beruht damit auf dem Prinzip **«naming and shaming»**. Wer sich nicht an die Empfehlungen der FATF hält, wird an den Pranger gestellt und muss mit Gegenmassnahmen respektive Schikanen durch die anderen Mitgliedstaaten rechnen. Gleiches gilt auch betreffend der Egmont Gruppe. Das Nichtbefolgen der Egmont Prinzipien kann zum Ausschluss aus der Egmont Gruppe führen, wodurch auch die FATF-Empfehlung 29 betroffen ist bzw. eine Verletzung des FATF-Standards vorliegt.

18 Die Schweiz gehört weltweit zu den führenden Finanzplätzen. Auf den Finanzsektor entfällt ein Siebtel der Schweizer Bruttowertschöpfung.[32] Rund zehn Prozent aller Arbeitsplätze in der Schweiz sind direkt oder indirekt vom Finanzsektor abhängig.[33] Der Schweizer Finanzplatz bildet einen wichtigen Eckpfeiler der Schweizer Wirtschaft. Die Attraktivität des Finanzplatzes Schweiz baut auf einem reibungslos funktionierenden Finanzdienstleistungsangebot und einem einwandfreien Ruf auf. Allfällige Gegenmassnahmen von anderen Staaten wirken sich negativ auf den Schweizer Finanzplatz und somit die Schweizer Wirtschaft aus. Die Verletzung des FATF-Standards und der Egmont Prinzipien gilt es somit zu vermeiden. Im Interesse eines funktionierenden und glaubwürdigen Finanzplatzes ist die Schweiz somit **de facto gezwungen,** Soft Law im Bereich der Finanzmarktregulierung ins nationale Recht zu transformieren.

III. REGELUNGSINHALT

A. Organisation – Die Meldestelle als Teil der fedpol (Abs. 1)

1. Eingliederung der Meldestelle in fedpol

19 Basierend auf ihren Aufgaben und Kompetenzen ist die Meldestelle eine **administrative Verwaltungsbehörde**[34] mit besonderen Aufgaben, wobei sie über keine polizeilichen Kompetenzen – namentlich Zwangsmassnahmen – verfügt.[35] Ihre Kompetenzen liegen in der Analyse und Beurteilung von gemeldeten und eingeholten Informationen.[36] Die Meldestelle ist weder Polizei- noch Justizbehörde, sie ist jedoch bei fedpol angegliedert.

20 Gemäss Abs. 1 führt das Bundesamt für Polizei fedpol die Meldestelle für Geldwäscherei. In der französischen Gesetzesübersetzung heisst es «gérer», was eher die Bedeutung von «verwalten» hat. Was unter **«führen»** bzw. **«gérer»** gemeint ist, wird in Gesetz und Verordnung nicht weiter ausgeführt. Die Frage der Unterstellung und damit des Grades der Unabhängigkeit der Meldestelle ist relevant. Im Wesentlichen geht es darum, dass eine FIU in ihren operativen Kernprozessen unabhängig sein muss und bei ihren Fallanalysen selbstständig entscheidet, ob und was sie an die Strafverfolgung sowie weitere nationale und internationale Behörden übermittelt. Ebenso muss der Quellenschutz der Meldenden jederzeit gewährleistet sein. Eine entsprechende Trennung respektive Emanzipation von fedpol und der restlichen Zentralverwaltung ist deshalb erforderlich.

---

31. KV-KO-Ackermann/Zehnder, Art. 305bis StGB N. 49.
32. Ca. CHF 108.4 Mrd., vgl. BAK Economics, S. 5.
33. Ca. 479 000 Vollzeitbeschäftigte, vgl. BAK Economics, S. 5.
34. Es gibt verschiedene Arten von FIUs: administrative FIUs, polizeiliche FIUs, gerichtliche FIUs und gemischte FIUs. Für eine ausführliche Darstellung vgl. IMF/WB, FIUs – An Overview, S. 10–19).
35. Botschaft GwG 2012, S. 6948, S. 6969.
36. OFK-Thelesklaf, Art. 23 GwG N. 2.

21 Die EFK hält in ihrem Bericht vom 20. Dezember 2021 dazu fest: Die Frage der Unabhängigkeit sollte **nicht zu absolut** interpretiert werden. Schliesslich sei es sinnvoll, wenn die Meldestelle und die übrigen Bereiche von fedpol bei der Geldwäschereibekämpfung eng zusammenarbeiten. So habe es auch der Gesetzgeber gesehen, als er die Meldestelle dem damaligen BAP (Bundesamt für Polizei, heute fedpol) zugeordnet hatte. Die Meldestelle könne von der Infrastruktur von fedpol profitieren. Dieses Modell sei günstiger als der Unterhalt einer administrativ unabhängigen Einheit. Die Meldestelle erhalte von fedpol die finanziellen und personellen Mittel, die sie für die Erledigung ihrer Kernprozesse brauche. Die EFK sprach indessen die Empfehlung an fedpol und die Meldestelle aus, eine Geschäftsordnung ähnlich derjenigen der Internen Revision der Departemente und Ämter zu erarbeiten und die Frage, was das «Führen» von MROS durch fedpol gemäss Art. 23 Abs. 1 GwG beinhalte, abschliessend zu beantworten.[37]

22 fedpol und die Meldestelle haben die Empfehlung der EFK im Jahr 2022 umgesetzt und ein **Geschäftsreglement** erlassen. Im Jahresbericht der Meldestelle für das Jahr 2022 wird hierzu ausgeführt: *«Die Herausforderung bestand darin, die Abgrenzung der Aufgaben zwischen fedpol und der MROS so bestimmt wie möglich aufzuzeigen, um den Anforderungen von FATF und der Egmont-Gruppe bestmöglich gerecht zu werden. Im Gegenzug durfte die allgemeine Verwaltungsorganisation respektive die klar im Gesetz verankerte organisatorische und hierarchische Eingliederung der MROS in fedpol durch ein Reglement nicht ausgehebelt werden. Mit anderen Worten: Eine Geschäftsordnung/Reglement muss im Korsett der allgemeinen Verwaltungsorganisation Platz finden.»*[38] Die per 1. November 2022 in Kraft getretene Geschäftsordnung stützt sich auf vier zentrale Pfeiler:

23 Ziff. 1 – **Organisation**: Die Meldestelle ist als Abteilung organisatorisch und hierarchisch beim Direktionsbereich Kriminalprävention und Recht (KPR) angegliedert. Der Leiter Meldestelle übt die Leitung sowie Kontrolle und Aufsicht über die operative Geschäftsführung der MROS aus. Als Teil von fedpol untersteht die Meldestelle sämtlichen organisatorischen, personellen und verwaltungsrechtlichen Bestimmungen und Weisungen der allgemeinen Bundesverwaltung, des EJPD und von fedpol.[39]

24 Ziff. 2 – **Operative Aufgaben der Meldestelle**: Hauptaufgabe bildet das Meldewesen – die Entgegennahme von Verdachtsmeldungen, die Analyse und die Weitergabe der Informationen an die zuständigen Strafverfolgungsbehörden sowie die nationale und internationale Amtshilfe. Darüber hinaus ist die Meldestelle Mitglied der Egmont Gruppe, nimmt die damit verbundenen Rechte und Pflichten wahr, d.h. sie nimmt an den erforderlichen Meetings sowie Arbeitsgruppen und Expertenpanels teil, pflegt aktive Beziehungen zu den FIUs im Ausland und ist befugt, eigenständig Memorandum of Unterstandings (MoUs) mit den ausländischen Partnerstellen abzuschliessen. Des Weiteren figuriert die Meldestelle auch als die Fachstelle für die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung und widmet sich einer Reihe von präventiven Aufgaben (Sensibilisierung der Finanzintermediäre, Mitarbeit in Expertengruppen, Durchführung von Schulungen und Weiterbildungen etc.). Sie betreibt strategische Analyse und teilt und veröffentlicht ihre Erkenntnisse mit anderen Behörden, der Finanzbranche sowie Dritten. Die Meldestelle unterhält ein eigenes Datenbearbeitungssystem.[40]

25 Ziff. 3 – **Operationelle Unabhängigkeit** der Meldestelle: Die Meldestelle entscheidet autonom über die Art und Weise der Erfüllung und der Priorisierung der unter Ziff. 2 definierten Aufgaben. Sie entscheidet über den Einsatz der ihr zur Verfügung gestellten personellen Ressourcen. Ebenfalls setzt

37. Bericht EFK, S. 18 f.
38. Jahresbericht MROS, 2022, S. 11 f.
39. Geschäftsordnung fedpol/MROS, Ziff. 1.
40. Geschäftsordnung fedpol/MROS, Ziff. 2.

sie eigenständig thematische Schwerpunkte (Triage, Priorisierung etc.). In Bezug auf die Thematik der finanziellen und personellen Ressourcen weist die Geschäftsordnung darauf hin, dass fedpol diese für die von der Meldestelle zu erfüllenden Aufgaben bereitstellt, wobei die Organisations- und Budgetvorgaben der Bundesverwaltung einzuhalten sind. Weitere Punkte dieser Regelung betreffen die Themen der Anstellung von Mitarbeitenden, den Informationsschutz und die Reisetätigkeit.[41]

26 Ziff. 4 – **Prüfung der operativen Unabhängigkeit**: Abschliessend enthält die Geschäftsordnung Regelungen zur Überprüfung und Eskalation. Demnach prüft das Finanzinspektorat des Generalsekretariats des Justiz- und Polizeidepartements (FISP)[42] die operationelle Unabhängigkeit der Meldestelle periodisch, verfasst darüber einen Bericht und spricht gegebenenfalls Empfehlungen aus. Weiter ist die FISP auch Beurteilungsinstanz bei Unklarheiten in Bezug auf Unabhängigkeitsfragen.[43]

27 Mit der Geschäftsordnung verfügen die Meldestelle und fedpol nun über **klare Abgrenzungskriterien** hinsichtlich der Tätigkeit der Meldestelle. Der Erlass der Geschäftsordnung wurde in einem Audit der Egmont Gruppe, welcher im Jahr 2022 stattgefunden hat, als positiv beurteilt.[44]

2. Umsetzung der internationalen Vorgaben ins nationale Recht

28 Die FATF hat die Schweiz 2016 zum vierten Mal geprüft und im Jahr 2020 einen Follow-up durchgeführt.[45] In beiden Berichten hielt die FATF fest, dass die Meldestelle **konform** mit der Empfehlung 29 zur operativen Unabhängigkeit ist. Auch die EFK kam in ihrem Bericht zu einem ähnlichen Ergebnis: *«Die Meldestelle ist angemessen in die Strukturen und Prozesse von fedpol eingebunden. Die EFK hat keine Situation identifiziert, wo fedpol die erforderliche, operative Unabhängigkeit von MROS verletzte.»*[46]

29 Einzig die Egmont Gruppe äusserte ihm Rahmen ihres im Jahr 2022 durchgeführten On-Site-Reviews punkto Unabhängigkeit eine **gewisse Kritik**. Zwar kam auch sie zum Schluss, dass die Meldestelle mit den entsprechenden Egmont Prinzipien «compliant» sei. Sie hat jedoch auch angeführt, dass die fehlende Budgetkompetenz der Meldestelle, die fehlende eindeutige Zuweisung von personellen Ressourcen zugunsten der Meldestelle sowie das Fehlen von konkreten Regeln für die Berufung und Abberufung des Leiters der Meldestelle unter dem Gesichtspunkt der Unabhängigkeit einer FIU als problematisch einzustufen seien. Dies berge ein notorisches Konfliktpotential zwischen Meldestelle und fedpol.[47]

30 Die Frage der Unabhängigkeit wird im Rahmen der anstehenden 5. Länderprüfung der FATF, welche von Ende 2026–2028 durchgeführt wird, erneut Thema sein. Im Unterschied zur letzten Länderprüfung im Jahr 2016 wird hierbei der Fokus nicht nur auf der technischen Umsetzung der Empfehlung 29 ins nationale Recht liegen, sondern vielmehr auf der **Effektivität**. Die operative Unabhängigkeit wird demnach an den Aktivitäten der Meldestelle, insbesondere an der freien Interaktion der Meldestelle mit anderen nationalen Behörden, ausländischen Partnerstellen und der Finanzindustrie gemessen werden.[48]

---

41. Geschäftsordnung fedpol/MROS, Ziff. 3.
42. Das FISP ist die interne Revisionsstelle des EJPD und der diesem unterstellten Verwaltungseinheiten im Sinn von Art. 11 des Bundesgesetzes über die Eidgenössische Finanzkontrolle (FKG, SR 614.0).
43. Geschäftsordnung fedpol/MROS, Ziff. 4.
44. Jahresbericht MROS, 2022, S. 11 f. (Kap. 2.3.1).
45. Vgl. hierzu die entsprechenden Berichte: MER 2016 und FUR 2020.
46. Bericht EFK, S. 19.
47. Addendum und Bericht der Egmont Gruppe im Rahmen ihres 2021/2022 durchgeführten On-Side-Reviews (nicht öffentlich zugänglich).

B. Die Analyse von Verdachtsmeldungen – «Intelligence» (Abs. 2)

1. Grundsatz

31 Kernaufgabe der Meldestelle ist die **Analyse** der eingehenden Verdachtsmeldungen. Meldepflichtig und/oder -berechtigt sind Finanzintermediäre gemäss Art. 2 GwG,[49] die im Kontext der Geldwäscherei- und Terrorismusfinanzierung betrauten Aufsichtsbehörden (FINMA, ESBK, BAZG, GESPA)[50] und parastaatlichen Aufsichtsinstanzen (SROs[51] und Aufsichtsorganisationen[52]) sowie Händler nach Art. 2 Abs. 1 lit. b i.V.m. 8a GwG und deren Revisionsstellen (vgl. Art. 1 Abs. 2 lit. a MGwV). Der Kreis der Meldenden ist damit beschränkt. Eine Meldemöglichkeit für Dritte (z.B. besorgte Bürger, Unternehmen, Medien etc.) besteht nicht – die Meldestelle ist nicht ermächtigt, Anzeigen von solchen entgegenzunehmen und inhaltlich zu behandeln.[53]

32 Die Schweiz hat ein **qualitatives Meldewesen**, d.h. eine Verdachtsmeldung beruht auf einem begründeten Verdacht und nicht auf quantitativen Schwellenwerten, deren Überschreitung eine automatische Übermittlung an die Meldestelle auslöst. Die Finanzintermediäre und die weiteren Meldepflichtigen sind integrierender Bestandteil des Verdachtsmeldesystems, indem sie potentiell verdächtige Transaktionen prüfen, bewerten und inhaltlich aufbereiten, bevor sie diese an die Meldestelle übermitteln. Die Meldestelle soll nicht mit unzureichend begründeten Verdachtsmeldungen überschwemmt werden.[54] Es darf somit bei den Meldenden vorausgesetzt werden, dass die minimalen formellen Anforderungen gemäss Art. 3 und 3a MGwV eingehalten werden und die übermittelten Sachverhalte eine gewisse inhaltliche Substantiierung aufweisen (vgl. Art. 3 Abs. 1 lit. h MGwV). Die Meldestelle weist formell fehlerhafte und unbegründete Verdachtsmeldungen zur Verbesserung zurück.[55] Sie bestätigt den Eingang einer Verdachtsmeldung erst nach Erhalt aller Informationen und Dokumente gemäss Art. 3 und 3a MGwV – eine Verdachtsmeldung gilt somit erst dann als eingereicht, wenn die Empfangsbestätigung durch die MROS ausgestellt wurde.

33 Primäres Ziel der Analysetätigkeit der Meldestelle ist es zu klären, ob sich der Verdacht, der zur Meldung geführt hat, erhärtet oder nicht. Weiter besteht der Anspruch, die nachgelagerten Strafverfolgungsbehörden mit konzisen Analyseberichten zu unterstützen und zu entlasten, sprich **Mehrwerte** – Financial Intelligence – zu generieren. Bei dieser sogenannten operativen Analyse werden verfügbare und beschaffbare Informationen verwendet, um bestimmte Ziele (z.B. Personen, Vermögenswerte, kriminelle Netzwerke und Vereinigungen) zu ermitteln, Spuren bestimmter Aktivitäten oder Transaktionen zu verfolgen und Verbindungen zwischen diesen Zielen und möglichen Erträgen aus Straftaten, Geldwäscherei, Vortaten oder Terrorismusfinanzierung festzustellen. Ausgangspunkt bildet dabei immer eine Verdachtsmeldung eines Finanzintermediärs oder eine Anzeige (Spontaninformation oder Anfrage) einer internationalen Partnerstelle

48. Vorstellung der Methodologie der FATF für die 5. Länderprüfung anlässlich des Joint Assessor Trainings (JAT) der FATF vom 4.–8.3.2024 in Hong Kong.
49. Meldepflicht gestützt auf Art. 9 Abs. 1 GwG. Melderecht basierend auf Art. 305ter Abs. 2 StGB.
50. Meldepflicht gestützt auf Art. 16 Abs. 1 GwG.
51. Meldepflicht gestützt auf Art. 27 Abs. 4 GwG.
52. Meldepflicht gestützt auf Art. 16 Abs. 1 GwG.
53. Einzige Ausnahme bilden Meldungen betreffend unrechtmässig erworbene Vermögenswerte ausländischer politisch exponierter Personen nach Art. 7 Abs. 1 und 2 SRVG. Diese Meldungen können von allen Personen und Institutionen erstattet werden, die aus irgendeinem Grund mutmasslich unrechtmässig erworbene Vermögenswerte von politisch exponierten Personen oder ihnen nahestehenden Personen halten, betreuen oder verwalten (vgl. hierzu BSK-Berger, Art. 23 N. 21, m.w.A., und Verweis auf Botschaft SRVG 2014, S. 5309).
54. Botschaft GwG 2019, S. 5479.
55. Jahresbericht MROS, 2022, S. 16 (Ziff. 3.3).

(ausländische FIU).[56] Es bedarf somit einer **Triggerinformation**. Die Meldestelle hat keine Kompetenz, von sich aus tätig zu werden – zum Beispiel aufgrund von Medienberichten.

34 Sofern eine Triggerinformation vorliegt, kann die Meldestelle den **«roten Faden»** aufnehmen, die im eigenen Datenverarbeitungssystem goAML vorhandenen Informationen nutzen und die Instrumente zur weiteren Informationsbeschaffung einsetzen. Zentral sind hier die Möglichkeiten gemäss Art. 11a GwG, beim meldenden Finanzintermediär und bei mutmasslich involvierten Drittinstituten zusätzliche Informationen einzuholen. Darüber hinaus bestehen aber noch weitere Instrumente der Informationsbeschaffung, wie die nationale Amtshilfe, das Abrufen von Informationen in Justiz- und Polizeidatenbanken,
das Beschaffen von Informationen über das Egmont-Netzwerk sowie OSINT (vgl. Ziff. III.B.2 hiernach).

35 Der FATF-Standard verlangt, dass die MROS nebst der operativen auch die **strategische Analyse** betreibt. Bei der strategischen Analyse werden verfügbare und beschaffbare Informationen, einschliesslich Daten, die von anderen Behörden bereitgestellt werden können, verwendet, um Trends, Methoden und Muster im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung zu ermitteln. Diese Informationen werden dann verwendet, um Bedrohungen und Schwachstellen im Abwehrdispositiv zu ermitteln und Gegenmassnahmen auszulösen. Dabei beschränkt sich der Nutzen nicht nur auf die MROS – die gewonnenen Informationen sollen den anderen Behörden und der Finanzindustrie gleichermassen dienen.

36 Die strategische Analyse ist in Art. 1 Abs. 2 lit. f MGwV verankert. Bis zur Anpassung der MGwV am 1. Januar 2016 enthielt weder das GwG noch die MGwV einen expliziten Verweis auf die strategische Analyse.[57] Die MROS betreibt heute strategische Analyse schwerpunktmässig im Bereich der Erstellung der **sektoriellen und nationalen Risikoanalysen**. Weiter werden auch punktuell Phänomene aufgearbeitet. Als Beispiel ist hier der «Alert» im Bereich der Terrorismusfinanzierung, welcher die Meldestelle zuhanden der Finanzbranche im Späterherbst/Winter 2023 adressiert hat, zu erwähnen.[58] Ab Januar 2025 plant die MROS mittels einer öffentlichen und webbasierten Typologiendatenbank, der Finanzbranche Fallkonstellationen anonymisiert zur Verfügung zu stellen. Ein weiteres Betätigungsfeld für strategische Analyse ist die Public Private Partnership (PPP), welche im November 2024 unter der Bezeichnung «Swiss FIPPP[59]» ihren operativen Betrieb aufgenommen hat. Letztere ist auf den Austausch von Informationen im Bereich Trends, Methoden und Typologien ausgerichtet.[60]

2. Instrumente der Analyse – «Toolbox» der Meldestelle

37 Damit die MROS im Rahmen ihrer Analysen der Verdachtsmeldungen möglichst **holistische Bilder** der mutmasslich inkriminierten Transaktionen und involvierten Netzwerke aufzeigen kann, braucht sie nebst der auslösenden Verdachtsmeldung möglichst viele **zusätzliche Informationsquellen**. Die

56. Botschaft GwG 2018, S. 6507 f.
57. Vgl. SHK-Derungs/Gmünder, Art. 23 GwG N. 19.
58. Alerts and typologies in the context of the terrorist attacks by Hamas and Palestinian Islamic Jihad (PIJ) on Israel on October 7, 2023 https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/alerts-and-typologies.pdf.download.pdf/alerts-and-typologies.pdf und Addendum to the alert dated November 3, 2023 in the context of the terrorist attacks by Hamas and Palestinian Islamic Jihad (PIJ) on Israel on October 7, 2023 https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/addendum-to-alert.pdf.download.pdf/addendum-to-alert.pdf, beide besucht am 30.11.2024.
59. Swiss Financial Intelligence Public Private Partnership; vgl. auch Webseite: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/swiss-fippp.html, besucht am 30.11.2024.
60. https://www.fedpol.admin.ch/fedpol/de/home/aktuell/mm.msg-id-103066.html, besucht am 30.11.2024; vgl. auch Jahresbericht MROS, 2023, S. 12.

MROS hat auf zwei verschiedene Arten Zugang zu bestimmten Zusatzinformationen. Erstens besitzt sie einen Zugriff auf mehrere Datenbanken. Zweitens kann sie Finanzintermediäre sowie in- und ausländische Behörden unter gewissen Voraussetzungen um Informationen ersuchen.[61]

a. Informationen der Finanzintermediäre

38 Nebst der Ausgangsinformation – der Verdachtsmeldung – sind auch die weiteren **Finanzinformationen**, welche die Meldestelle gestützt auf Art. 11a GwG beim meldenden Finanzintermediär und bei Drittintermediären herausverlangen kann, wesentliche Elemente einer Transaktionsanalyse. Kriminelle Netzwerke sind heute international mit Schachtelstrukturen und institutsübergreifend präsent. Damit ein (möglichst) vollständiges Bild erzeugt werden kann, ist es für die Meldestelle unabdingbar, die vollständigen Informationen, die bei den Finanzintermediären vorhanden sind, abzurufen und in der Analyse zu berücksichtigen. Die Meldestelle kann heute in **drei Konstellationen** Informationen bei den Finanzintermediären einholen:

39 Art. 11a Abs. 1 GwG gibt der Meldestelle die Möglichkeit beim **meldenden Institut** zusätzliche Informationen einzuholen. Die Herausgabepflicht erstreckt sich auf sämtliche Informationen, welche die Meldestelle für ihre Analyse benötigt und die beim **Finanzintermediär** vorhanden sind. Als verfügbare Informationen gelten solche, welche in den – der Schweizer Jurisdiktion unterliegenden – Entitäten eines Unternehmens vorhanden sind oder beschafft werden können.[62] Nach der hier vertretenen Meinung geht der Herausgabeanspruch der Meldestelle über das blosse Nachfordern von Informationen von unvollständig eingereichten Verdachtsmeldungen hinaus.[63] Dies ergibt sich bereits aus dem klaren Wortlaut der Gesetzesbestimmung und auch aus der FATF-Empfehlung 29, welche von «additional information from reporting entities» spricht. Darüber hinaus muss es der Meldestelle jedoch bereits basierend auf einer von ihr initiierten Analyse – welche dann eben auch Informationen aus anderen Quellen und nicht nur Informationen aus der Verdachtsmeldung beinhaltet – möglich sein, beim meldenden Institut zusätzliche Informationen einzufordern. Eine andere Interpretation würde der Aufgabe der Meldestelle, vertiefte Analysen durchzuführen, zuwiderlaufen.

40 Art. 11a Abs. 2 GwG sieht vor, dass die Meldestelle auch beim **Drittintermediär** Informationen herausverlangen kann, wenn aufgrund der Analyse erkennbar wird, dass dieser an der untersuchten Transaktion oder Geschäftsbeziehung in irgendeiner Form beteiligt ist oder war. Voraussetzung ist, dass der Anhaltspunkt für die Betroffenheit des Drittintermediärs aus einer bei der MROS eingegangenen Verdachtsmeldung stammt. Der Umfang der Herausgabepflicht von Abs. 2 deckt sich mit Abs. 1.[64]

41 Art. 11a Abs. 2bis GwG sieht schliesslich vor, dass die Meldestelle auch aufgrund von Informationen ihrer **ausländischen Partnerbehörden** bei den Finanzintermediären Informationen einfordern kann. Dabei spielt es keine Rolle, ob es sich bei den Informationen der ausländischen FIU um ein Ersuchen oder eine Spontaninformation handelt. Weiter ist auch unerheblich, ob im gleichen Kontext vorgängig bereits eine Verdachtsmeldung von einem Meldepflichtigen bei der Meldestelle eingegangen ist. Auch bei Abs. 2bis ist der Umfang der Herausgabepflicht mit Abs. 1 und Abs. 2 deckungsgleich.[65]

---

61. Botschaft GwG 2014, S. 633.
62. Botschaft GwG 2012, S. 6972; BSK-Naegeli, Art. 11a GwG N. 20 und 24; SHK-Luchsinger, Art. 11a GwG N. 15 f.; OFK-Thelesklaf, Art. 11a GwG N. 2.
63. KV-KO-Hutzler, Art. 11a GwG N. 8; **a.M**. SHK-Luchsinger, Art. 11a GwG N. 15 f. und BSK-Naegeli, Art. 11a GwG N. 21 ff.
64. BSK-Naegeli, Art. 11a GwG N. 34.
65. Botschaft Verhütung Terrorismus 2018, S. 6507 ff.; BSK-Naegeli, Art. 11a GwG N. 38 ff.

b. Zugriff auf Polizei- und Justizdatenbanken

42 Für die operationelle Analyse von Verdachtsmeldungen stützt sich die Meldestelle primär auf ihre eigene Datenapplikation goAML, d.h. es wird in den eigenen Daten nach Verknüpfungen und weiteren Anhaltspunkte gesucht, die dann zu weiteren Analyseschritten und Abfragen führen. Darüber hinaus verfügt die Meldestelle aber auch über Zugriffsrechte zu verschiedenen **behördlichen Datenbanken**, um zu überprüfen, ob die in den erhaltenen Informationen erwähnten natürlichen und juristischen Personen bereits behördlich bekannt sind.

43 Art. 35a Abs. 1 GwG legitimiert die Meldestelle, auf die folgenden polizeilichen und justiziellen Datenbanken im **Abrufverfahren** zuzugreifen und zu überprüfen, ob die fraglichen Personen verzeichnet sind («Hit/No-Hit): (1) Nationaler Polizeiindex; (2) Zentrales Migrationssystem (ZEMIS); (3) Automatisiertes Strafregister (VOSTRA); (4) Staatsschutz-Informationssystem (ISIS – überführt in IASA INDEX [NDB]); (5) Personen-, Akten- und Geschäftsverwaltungssystem im Bereich der Rechtshilfe für Strafsachen (TROVA).

44 Art. 35 Abs. 2 GwG ermöglicht der Meldestelle **weitergehende Zugriffe** auf die in Abs. 1 erwähnten Informationssysteme, soweit die auf das jeweilige Informationssystem anwendbaren Bestimmungen dies vorsehen.[66] So kann die Meldestelle beispielsweise auf sämtliche im Polizeiindex enthaltenen Informationen zugreifen.[67] Für ZEMIS[68] und VOSTRA[69], IASA INDEX (NDB)[70] und TROVA[71] gelten spezifische respektive unterschiedliche Einsichtsrechte, d.h. es kann jeweils nur auf einen Teil der Daten zugegriffen werden.

45 Darüber hinaus kann die Meldestelle auf weitere Informationssysteme aufgrund **spezialgesetzlicher Grundlagen** zugreifen (z.B. RUMACA[72]). Derzeit bestehen Zugriffsrechte in unterschiedlicher Ausprägung auf 15 polizeiliche und justizielle Datenbanken.

c. Informationen aus der internationalen Amtshilfe

46 Eine wesentliche Informationsquelle für die operativen Analysen der Meldestelle sind die ausländischen Partnerstellen (FIUs). Ein Grossteil der Verdachtsmeldungen hat einen internationalen Konnex.[73] Die Meldestelle kann hier **Anfragen an die ausländischen FIUs** stellen. Ebenfalls profitiert sie von eingehenden Spontaninformationen und Anfragen, welche oftmals wertvolle Anhaltspunkte und Hinweise enthalten und somit eine bereits laufende Analyse vorantreiben können. Der Informationsaustausch zwischen der Meldestelle und ihren ausländischen Pendants richtet sich nach Art. 30 GwG sowie den Egmont Prinzipien.[74] Beim Austausch von Informationen sind in jedem Fall die Prinzipien der Spezialität (nur zu Analysezwecken), der Reziprozität (Gegenseitigkeit) und der Vertraulichkeit zu berücksichtigen.[75] Weiter unterliegen die erhaltenen Informationen einem Disseminationsvorbehalt, d.h. die ausländische Behörde bestimmt, an wen die Informationen weitergeleitet werden dürfen.[76]

---

66. BSK-Gaul/Isler/Vasella, Art. 35 GwG N. 3 ff., m.w.H.
67. Art. 17 Abs. 4 und 5 BPI und Art. 4 und 5 Abs. 1 lit. e und Abs. 3 (Verweis auf Anhang) Polizeiindex-Verordnung (SR 361.4).
68. Art. 4 ZEMIS-Verordnung (SR 142.513) mit Verweis auf Anhang.
69. Art. 46 StReG (SR 330).
70. Anhang 3 VIS-NDB (SR 121.2).
71. Art. 11a Abs. 3 IRSG (SR 351.1) i.V.m. Art. 10 Abs. 1 lit. e ELPAG-Verordnung (SR 351.12).
72. Anhang 4 DBZV (SR 631.061).
73. Jahresbericht MROS, 2023, S. 31 (Ziff. 4.14) m.w.H.
74. Die MROS wendet die Egmont Principles analog – im Sinne eines Mindeststandards – auch auf Nichtmitglieder der Egmont Gruppe an.
75. Art. 30 Abs 1 GwG; vgl. hierzu Ordolli, S. 1409.
76. Egmont Principles Exchange, Art. 32.

d. Informationen aus der nationalen Amtshilfe

47 Auch Informationen aus der nationalen Amtshilfe können das Bild einer Analyse komplettieren oder eine solche erst ermöglichen. Die Meldestelle verzeichnet hier seit 2020 eine stetige Zunahme an Informationen.[77] Grundsätzlich ist ein **Austausch mit jeder Schweizer Behörde** möglich, sofern die Voraussetzungen gemäss Art. 29, 29a und 29b GwG erfüllt sind.

48 Art. 29 Abs. 1 und 29b GwG regeln die nationale Amtshilfe zwischen der Meldestelle und den verschiedenen **Aufsichtsbehörden und -instanzen**. Die im Gesetz genannten Behörden können einander «alle Auskünfte» erteilen, welche sie für die «Anwendung des GwG» benötigen. Es handelt sich hierbei um eine **Kann-Bestimmung**. Die jeweils von der Anfrage der Meldestelle betroffene Behörde entscheidet selbständig, ob sie die einverlangten Informationen zur Verfügung stellt.

49 Art. 29 Abs. 2 GwG sieht vor, dass die Meldestellte bei **sämtlichen Schweizer Behörden** Informationen erhältlich machen kann, die sie für die Analysen im Kontext zu Geldwäscherei, deren Vortaten, organisierter Kriminalität oder Terrorismusfinanzierung benötigt.[78] Dazu gehören nebst Finanzinformationen auch Informationen in Bezug auf Straf-, Verwaltungsstraf- und Verwaltungsverfahren, einschliesslich solcher aus hängigen Verfahren. Im Unterschied zu Abs. 1 besteht hier eine **Herausgabepflicht** zulasten der ersuchten Behörden.[79] In der Praxis sind aber gerade kantonale und kommunale Behörden sehr zurückhaltend mit der Herausgabe von Informationen. Der Art. 29 Abs. 2 GwG ist ihnen wenig geläufig.

50 Art. 29a GwG verlangt schliesslich, dass die Strafbehörden der Meldestelle sämtliche Verfügungen, die aufgrund einer Anzeige gestützt auf Art. 23 Abs. 4 GwG erlassen wurden, zustellt. Weiter verlangt die Bestimmung, dass die Meldestelle über hängige Verfahren informiert wird und ihr **Urteile und Einstellungsverfügungen** samt Begründung zugestellt werden, sofern denn ein Konnex zu Geldwäscherei, ihrer Vortaten, organisierter Kriminalität oder Terrorismusfinanzierung vorliegt.

e. OSINT und weitere Informationsquellen

51 Im Zuge der globalen und kontinuierlich steigenden Verfügbarkeit von Daten und deren Vernetzung kommt bei Transaktions- und Netzwerkanalysen der Open Source Intelligence (OSINT) immer eine grössere Bedeutung zu. Unter OSINT versteht man das Sammeln, Analysieren und Verbreiten von Informationen aus **öffentlich zugänglichen Quellen**, mit Blick auf eine spezifische Fragstellung oder Analyse. OSINT-Quellen sind: Klassische Medien, Soziale Medien, Webseiten, Dark Web, kommerziell angebotene Datenbanken, behördliche Register, Archive, veröffentlichte Statistiken von Behörden und Privaten etc. Die Meldestelle nutzt heute gezielt auch OSINT-Informationen. Grundsätzlich kann die Meldestelle sämtliche öffentlich verfügbaren Informationen und Daten nutzen.[80] Die für die Meldestelle geltenden datenschutzrechtlichen Vorgaben und Einschränkungen sind gleichermassen auch auf OSINT anwendbar.

3. Risikobasierter Ansatz

52 Die Arbeitsweise der Meldestelle hat sich in den letzten Jahren stark verändert. Bedingt durch den drastischen Anstieg der Verdachtsmeldungen und des Reportingvolumens kann die Meldestelle nicht mehr alle Informationen im selben Detaillierungsgrad analysieren und weiterverarbeiten.[81] Die Meldestelle setzt **Prioritäten und Schwerpunkte**. Seit der Einführung der Datenapplikation goAML

77. Jahresbericht MROS, 2023, S. 31 (Ziff. 4.15).
78. SHK-Beuret, Art. 29 N. 21 ff.; BSK-Naegeli, Art. 29 N. 56 ff.
79. Botschaft GwG 2014, S. 692.
80. Art. 3 lit. a. ZentG.

per 1.1.2020 verfolgt die Meldestelle beim Empfang und bei der Bearbeitung von Verdachtsmeldungen einen **«risikobasierten Ansatz»**: Die eingehenden Verdachtsmeldungen werden mittels **«Triage-Matrix»** nach Risiko kategorisiert, priorisiert und dann basierend auf dieser Einteilung mit unterschiedlicher Ausprägung analysiert.[82] Die Meldestelle fokussiert auf die Bekämpfung von Schwerstkriminalität – die Schwerpunkte liegen auf der organisierten Kriminalität, der Terrorismusfinanzierung sowie bestimmten Formen der Wirtschaftskriminalität. Dabei orientiert sich die Meldestelle auch an den Strategien der Strafverfolgungsbehörden, operiert erfolgsorientiert und berücksichtigt potenzielle Reputationsrisiken für den Finanzplatz Schweiz.[83]

53 Im Jahr 2023 wurde eine von fünf Meldungen **tiefgreifend analysiert**. Die restlichen 80% der Verdachtsmeldungen wurden abgestuft oder mit gesamtheitlichen Analyseverfahren (z.B. Clusteringmethoden) bearbeitet. Ein Teil der Meldungen wurde bereits beim Empfang aussortiert, sog. «gefiltert». Dies bedeutet, dass die Meldung und die darin enthaltenen Informationen nicht mehr weiterverfolgt werden, jedoch für die spätere Verwendung in der Datenapplikation goAML zur Verfügung stehen. Die Meldestelle führt im Jahresbericht 2023 aus, dass ihre Analysen im Vergleich zu früher tendenziell mehr Informationen enthalten, d.h. sich aus verschiedenen Verdachtsmeldungen und zusätzlich eingeholten Informationen zusammensetzen und dadurch auch die Komplexität gestiegen ist. Ebenfalls konnten Verdachtsmeldungen, die bereits zu einem früheren Zeitpunkt gefiltert wurden, aufgrund später hinzugekommener Informationen wieder reaktiviert werden. Durch den risikobasierten Absatz bewegt sich die Meldestelle weg vom traditionellen Bearbeitungsansatz «1 Meldung gleich 1 Anzeige an die Strafverfolgungsbehörden» hin zu aktiver **«Intelligence»** und zur Vernetzung der vorhandenen Informationen. Nicht mehr die Verdachtsmeldung als solches, sondern deren Informationsgehalt steht im Mittelpunkt der Analyse.[84]

C. Informationssystem (Abs. 3)

1. Einsatz der Softwareapplikation «goAML»

54 Die Meldestelle ist zur Erfüllung ihrer Aufgaben zum Betrieb eines eigenen Datenbearbeitungssystems verpflichtet.[85] Seit dem 1.1.2020 ist die von der UNODC[86] entwickelte **Softwareapplikation goAML** im Einsatz, welche das Vorgängersystem GEWA[87] abgelöst hat. Die goAML-Anwendung ist eine vollständig integrierte Softwarelösung, die speziell für den Einsatz durch FIUs entwickelt wurde und heute weltweit in über 60 Länder im Einsatz steht.[88] Die Applikation wird von der UNODC kontinuierlich in Zusammenarbeit mit den FIUs weiterentwickelt und mit neuen Features ausgestattet. Die Meldestelle hat 2023 auf die Version 5.2. umgestellt; derzeit läuft für die Finanzintermediäre eine Übergangsfrist bis spätestens Ende 2024, um die nötigen Anpassungen an ihren Schnittstellen und Prozessen vorzunehmen.[89]

---

81. Die Anzahl der Verdachtsmeldungen haben sich seit 2014 verzehnfacht. Seit 2020 gar verdoppelt (vgl. Jahresbericht MROS 2023, S. 22 [Ziff. 4.2 und Abbildung 2]).
82. Vgl. Strategie MROS 2024–2027.
83. Basierend auf einer Matrix werden die Meldungen nach dem Empfang triagiert und priorisiert, wobei die folgenden Kriterien (nicht abschliessend und in unterschiedlicher Kombination) ausschlaggebend sind: Schwere der Vortrat, Höhe der Transaktionssumme, Höhe der betroffenen Assets, Qualität des Betroffenen (PEP, geografische Aspekte etc.), Aktualität, bestehende Hinweise in der goAML-Datenbank (Wiederholungsfall, Zusammenhänge, Muster etc.), Strategie der Strafverfolgungsbehörden, Erfolgschancen, Risiken für die MROS (Reputation) etc.
84. Jahresbericht MROS, 2023, S. 8 f. (Kap. 2.2).
85. Art. 23 Abs. 3 GwG i.v.m. Art. 1 Abs. 2 lit. 2 MGwV.
86. United Nations Office on Drugs and Crime.
87. GEWA war eine «Inhouse»-Eigenentwicklung des ISC-EJPD und ein reines Erfassungs- und Abfragesystem ohne Verarbeitungsmöglichkeiten oder -funktionen.
88. https://unite.un.org/goaml/, besucht am 30.11.2024.

55 goAML erlaubt die **elektronische Entgegennahme von Verdachtsmeldungen**. Den Finanzintermediären stehen dabei drei verschiedene Übermittlungswege offen: (1) Die vollständig automatische Übermittlung via XML-Datei, (2) eine semiautomatische Lösung, bei welcher nur die Konten und Transaktionen via XML-Datei übermittelt und die restlichen Informationen über ein Web-Interface eingegeben werden, sowie (3) die vollständig manuelle Eingabe der Daten über das Web-Interface.[90] Rund 60% der Meldungen werden vollständig XML-basiert übermittelt. Diese Übermittlungsart ist im Vergleich zu den anderen weniger fehleranfällig. 75% der von der Meldestelle beim Empfang zurückgewiesenen Verdachtsmeldungen beziehen sich auf manuelle Eingabefehler.[91] Auch Anfragen gemäss Art. 11a GwG können vollständig über goAML abgewickelt werden. Behördenseitig kann die Meldestelle ebenfalls über goAML kommunizieren. Sämtliche Anzeigen gemäss Art. 23 Abs. 4 GwG inklusive der Übermittlung der Analyseberichte an die Strafverfolgungsbehörden sowie ein Grossteil der ausgehenden Spontaninformationen gemäss Art. 29 GwG werden heute via den goAML-Kanal übermittelt.

2. Bearbeitungsgrundsätze

56 Der Einsatz eines Informationssystems ist **nicht Selbstzweck**, sondern orientiert sich am Aufgabenkatalog und den Kompetenzen der Meldestelle und soll ihr die Erfüllung der Aufgaben ermöglichen und erleichtern. Entsprechend kann das Informationssystem für die drei Kernaufgaben Intelligence, Kooperation (nationale und internationale Amtshilfe) sowie für die Prävention eingesetzt werden (Art. 14 MGwV). Die im Informationssystem gespeicherten Daten stammen aus den Informationsquellen, auf welche die Meldestelle zugreifen kann. Zur Hauptsache sind es die Verdachtsmeldungen und die Informationen aus den Anfragen gestützt auf Art. 11a GwG. Des Weiteren sind darin aber auch sämtliche Informationen, welche der nationalen und internationalen Amtshilfe entstammen, sowie die Abklärungen und Analysen der Meldestelle als solches enthalten (Art. 15 MGwV).

57 Die MROS bearbeitet **besonders schützenswerte Daten** im Sinne von Art. 3 DSG. Dabei werden Personendaten im Zusammenhang mit verdächtigen Transaktionen sowie natürlichen und juristischen Personen bearbeitet, gegen die ein Verdacht wegen Geldwäscherei, ihrer Vortaten, organisierter Kriminalität oder Terrorismusfinanzierung vorliegt (Art. 16 Abs. MGwV). Darüber hinaus können auch Informationen über Dritte im Informationssystem eingetragen werden, soweit diese dem Zwecke der Meldestelle dienlich sind (Art. 16 Abs. 2 MGwV).

58 Der Zugriff auf das Informationssystem ist ausschliesslich **Mitarbeitenden der Meldestelle** sowie systembedingt dem Wartungspersonal vorbehalten (Art. 20 MGwV). Dies entspricht der konsequenten Umsetzung des Unabhängigkeitserfordernisses gemäss FATF und der Egmont Gruppe.[92]

59 Die im Informationssystem gespeicherten Daten werden höchstens 10 Jahre ab dem Zeitpunkt der Erfassung durch die Meldestelle aufbewahrt und in der Folge einzeln gelöscht (Art. 28 Abs. 1 MGwV). Gleiches gilt auch für die von der MROS erstellten Abklärungen und Analysen.

D. Anzeige an die Strafverfolgungsbehörden (Abs. 4)

60 Kommt die Meldestelle aufgrund ihrer Analyse zum Schluss, dass ein Verdacht hinsichtlich Geldwäscherei, ihrer Vortaten[93], organisierter Kriminalität, Terrorismusfinanzierung oder mangelnder

89. Jahresbericht MROS, 2023, S. 20 (Ziff. 3).
90. Jahresbericht MROS, 2020, S. 13 (Ziff. 3.3); vgl. hierzu auch Fact Sheet goAML und goAML Web User Manual, jeweils in der neusten Version abrufbar auf der Webseite von fedpol/MROS: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html; besucht am 30.11.2024.
91. Jahresbericht MROS, 2022, S. 18 (Ziff. 3.3).

Sorgfalt bei Finanzgeschäften vorliegt, so ist sie verpflichtet, der **zuständigen Strafverfolgungsbehörde** unverzüglich Anzeige zu erstatten.

61 Als Strafverfolgungsbehörden qualifizieren Behörden gemäss Art. 12 StPO. Somit sind grundsätzlich Anzeigen an die **Staatsanwaltschaften aber auch die Polizei** möglich. In der Regel erstattet die Meldestelle ihre Anzeigen an die Staatsanwaltschaften, da nur diese über die Kompetenz verfügen, die gesetzliche Sperre gemäss Art. 10 GwG zu verlängern. Polizeibehörden sind hierbei auf ein Mitwirken der Staatsanwaltschaften angewiesen. In Anbetracht der kurzen Entscheidungsfrist von lediglich fünf Tagen[94] sind die Polizeibehörden kaum in der Lage, über die Aufrechterhaltung der Vermögenssperre rechtzeitig zu entscheiden.

62 Die **sachliche Zuständigkeit** richtet sich nach Art. 22 ff. StPO. Die kantonale Gerichtsbarkeit bildet die Regel, die Bundesgerichtsbarkeit die Ausnahme.[95] Die Delikte, die der Bundesgerichtsbarkeit unterstehen, sind als Katalog in Art. 23 Abs. 1 StPO und Art. 24 StPO aufgeführt. Davon erfasst sind die klassischen Staatsschutzdelikte, also Straftaten, die sich vornehmlich gegen den Bund richten oder dessen Interessen stark berühren.[96] Weiter fallen darunter auch komplexe interkantonale bzw. internationale Fälle von organisierter Kriminalität – einschliesslich Terrorismus und dessen Finanzierung, Geldwäscherei und Korruption. Im Rahmen einer fakultativen Bundeskompetenz sind auch Delikte im Bereich der Wirtschaftskriminalität mit gesamtschweizerischer oder internationaler Ausprägung von der Bundeskompetenz erfasst.[97]

63 Die Meldestelle bestimmt **eigenständig und abschliessend**, an welche Strafverfolgungsbehörde sie ihre Analyseberichte respektive Anzeige übermittelt. Die langjährige Praxis der MROS besteht darin, sich aus Praktikabilitätsgründen auf den Ort der Geschäftsbeziehung zu stützen, da der Begehungsort der geldwäschereirelevanten Handlung im Vordergrund steht. Ausserdem werden Informationen aus unterschiedlichen Verdachtsmeldungen, welche den gleichen Sachverhalt betreffen, in einem Analysebericht verarbeitet und an dieselbe Staatsanwaltschaft übermittelt. Dadurch wird ihr ein besserer Überblick über den erweiterten Sachverhalt verschafft, welcher als Beurteilungsgrundlage im Hinblick auf eine allfällige Verfahrenseröffnung dienen kann.[98]

64 Die Meldestelle nimmt **keine übermittelten Anzeigen oder Teile davon zurück**. Dieses Vorgehen könnte unter anderem zu praktischen Problemen im Zusammenhang mit der Vermögenssperre nach Art. 10 Abs. 1 GwG respektive mit den Mitteilungen an die Finanzintermediäre nach Art. 23 Abs. 5 GwG führen. Sollte sich eine Strafverfolgungsbehörde für eine Anzeige der MROS als unzuständig betrachten, so ist sie in Anwendung von Art. 39 Abs. 1 StPO auf die Einleitung eines Gerichtsstandsverfahrens mit der ihrer Ansicht nach zuständigen Staatsanwaltschaft verwiesen.

65 Der Vorgang der Anzeige gemäss Art. 23 Abs. 4 GwG ist grundsätzlich **einmalig und einseitig**. Sobald eine Anzeige erfolgt ist, stützt sich ein weiterer Austausch mit den Strafverfolgungsbehörden in derselben Sache auf Art. 29 GwG.[99] Namentlich dürfen die Anfragen der Staatsanwaltschaft dann nur nach den Grundsätzen der nationalen Amtshilfe beantwortet werden. Die MROS kann sich mit den Strafverfolgungsbehörden vor dem Erstatten einer Anzeige mündlich austauschen, um allfällige Zuständigkeitsfragen und Übermittlungsmodalitäten zu klären oder abzuwägen, ob eine Übermittlung überhaupt Sinn macht.

---

92. Interpretativnote zur FATF-Empfehlung 29 (E. [N. 10]).
94. Art. 10 Abs. 2 GwG.
95. Art. 22 StPO.
96. Art. 23 StPO.
97. Art. 24 StPO.
98. Jahresbericht MROS, 2022, S. 44. (Ziff. 6.2).
99. Siehe dazu auch BSK-Berger, Art. 23 GwG N. 63.

66 Bezüglich Umfang der Anzeige an die Strafverfolgungsbehörden hält Art. 8 Abs. 1 MGwV fest, dass die Informationen, welche die MROS übermittelt, keine Angaben darüber enthalten dürfen, wer die Meldung erstattet oder Auskünfte erteilt hat. Diese Bestimmung ist im Rahmen der Teilrevision der MGwV am 1. Januar 2020 in Kraft getreten, nachdem in der letzten Länderevaluation kritisiert wurde, der **Quellenschutz** seitens der MROS sei ungenügend.[100] Konsequenz dieser Einschränkung ist, dass sich die MROS seither bei einer Übermittlung an die Strafverfolgungsbehörden nicht mehr explizit zum Grad der Involvierung des Finanzintermediärs äussert, sondern in ihren Analyseberichten lediglich auf die betroffenen Konten und Transaktionen hinweist. Zwar lassen sich dadurch Rückschlüsse auf den Meldenden oder Auskunftsgebenden nicht vermeiden – die Strafverfolgungsbehörden benötigen jedoch einen minimalen Kontext, damit sie ihre Ermittlungen aufnehmen und die erforderlichen Handlungen – insbesondere Sperrung der Konten – vornehmen können. Der Quellenschutz ist somit nicht absolut zu verstehen, sondern erschöpft sich darin, dass die MROS der zuständigen Strafverfolgungsbehörde die erforderlichen Informationen offenlegen muss, damit diese ihre Tätigkeit überhaupt aufnehmen kann.

E. Mitteilung an den Finanzintermediär (Abs. 5)

67 Abs. 5 sieht vor, dass die Meldestelle den meldenden Finanzintermediär darüber informiert, wenn sie die von ihm gemeldeten Informationen an eine Strafverfolgungsbehörde übermittelt. Das gilt sowohl für die Meldungen gestützt auf die Meldepflicht (Art. 9 GwG) wie auch für die Meldungen gestützt auf das Melderecht (Art. 305ter Abs. 2 StGB). Diese Information an den Finanzintermediär löst nach Art. 10 Abs. 1 GwG in beiden Fällen eine **gesetzliche Sperrung** der gemeldeten Vermögenswerte während fünf Arbeitstagen aus, die vom Finanzintermediär vorzunehmen ist.

68 Der Abs. 5 in seiner jetzigen Form ist per 1.1.2023 in Kraft getreten. Zuvor war Abs. 5 mit einer 20-tägigen Bearbeitungsfrist gekoppelt, innert welcher die Meldestelle dem nach Art. 9 Abs. 1 lit. a GwG (Meldepflicht) meldenden Finanzintermediär melden musste, ob sie die Meldung an eine Strafverfolgungsbehörde weiterleitet oder nicht. Die MROS musste somit den Finanzintermediär über das **Schicksal seiner Meldung informieren**. Die Bereinigung von Art. 5 drängte sich aus mehreren Gründen auf:

69 Die Meldestelle war aufgrund der steigenden Verdachtsmeldungen schon seit mehreren Jahren **nicht mehr in der Lage, die 20-tägige Bearbeitungsfrist einzuhalten**. Die Zeit reichte besonders bei Verdachtsmeldungen nicht aus, die eine vertiefte Analyse erfordern und Auskunftsersuchen an ausländische FIUs oder Informationsanfragen an weitere Finanzintermediäre gemäss Art. 11a Abs. 2 GwG nach sich ziehen.[101]

70 Weiter war die Einhaltung der Bearbeitungsfrist mit Blick auf den von der MROS angewendeten Intelligence-Ansatz nicht mehr zeitgemäss. Erst die Abschaffung der Bearbeitungsfrist räumte der Meldestelle den notwendigen **Spielraum** ein, um Verdachtsmeldungen zu triagieren respektive zu priorisieren oder zurückzustellen und mit unterschiedlicher Tiefe und Fokus zu behandeln.[102]

71 Letztlich war auch die systematische Information, ob eine Übermittlung der Information an die Strafverfolgungsbehörden erfolgt ist oder nicht, wenig zielführend, da sie falsch interpretiert werden und den Finanzintermediär zu **falschen Schlussfolgerungen** verleiten konnte. So könnte ein Finanzintermediär aus der Nicht-Übermittlung etwa schliessen, dass seine Verdachtsmeldung unbegründet war oder dass die gemeldeten Vermögenswerte rechtmässiger Herkunft sind. Auch

100. MER 2016, S. 55 (N. 159); Erläuterungen Teilrevision MGwV 2019, S. 8 und 15 f.
101. Jahresbericht MROS, 2021, S. 40 (Kap. 6.1.2).
102. Botschaft GwG 2019, S. 5480.

könnte eine solche Mitteilung für einen Finanzintermediär allenfalls bei der Abwägung eine Rolle spielen, ob er die gemeldete Geschäftsbeziehung aufrechterhalten soll oder nicht. Indessen ist es falsch, aus dem Verzicht der Meldestelle, Informationen aus einer Verdachtsmeldung an eine Strafverfolgungsbehörde zu übermitteln, bestimmte Schlüsse zu ziehen. Nicht selten leitet die Meldestelle Informationen an eine ausländische Meldestelle weiter. In diesen Fällen erfolgt nicht zwingend eine Übermittlung an eine schweizerische Strafverfolgungsbehörde. Weiter kann eine gemeldete Information auch erst später in Kombination mit weiteren Informationen einen Verdacht begründen und damit eine Übermittlung an eine Strafverfolgungsbehörde rechtfertigen. Nach dem von der Meldestelle verfolgten Intelligence-Ansatz ist nicht die Verdachtsmeldung als solches, sondern die darin enthaltenen Informationen ausschlaggebend. Daher sollten Finanzintermediäre aus einer Nicht-Übermittlung keine falschen Schlüsse ziehen, weder zur Angemessenheit ihrer Meldung noch zur rechtmässigen Herkunft der gemeldeten Vermögenswerte.[103]

72 Mit der **Bereinigung** von Abs. 5 wurde gleichzeitig auch aAbs. 6 gestrichen.[104] Die Informationspflicht der Meldestelle an die Finanzintermediäre wurde dadurch vereinheitlicht respektive Meldungen nach Art. 9 GwG und Art. 305ter Abs. 2 StGB einander gleichgestellt.

LITERATURVERZEICHNIS

Ackermann Jürg-Beat/Zehnder Stephanie, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen: Einziehung, Kriminelle Organisationen, Finanzierung des Terrorismus, Geldwäscherei, Band II, Zürich/Basel/Genf 2018 (zitiert KV-KO-Ackermann/Zehnder).

BAK Economics, Volkswirtschaftliche Bedeutung des Schweizer Finanzsektors – Studie im Auftrag der Schweizerischen Bankiervereinigung SBVg und des Schweizerischen Versicherungsverbandes SVV, Ergebnisse 2024, abrufbar unter https://www.svv.ch/sites/default/files/202411/BAK_Economics_Bedeutungsstudie_Finanzsektor_2024.pdf (zitiert BAK Economics).

Berger Corinne, Kommentierung zu Art. 23 GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Beuret Arnaud, Kommentierung zu Art. 29 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Derungs Corsin/Gmünder Eliane, Kommentierung zu Art. 23 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Gaul Caroline/Isler Michael/Vasella David, Kommentierung zu Art. 35a GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Hutzler Doris, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen: Einziehung, Kriminelle Organisationen, Finanzierung des Terrorismus, Geldwäscherei, Band II, Zürich/Basel/Genf 2018 (zitiert KV-KO-Hutzler).

International Monetary Fund & World Bank, Financial Intelligence Units – An Overview, Washington D.C. 2004, abrufbar unter https://doi.org/10.5089/9781589063495.069 (zitiert IMF/WB, FIUs – An Overview).

103. Jahresbericht MROS, 2021, S. 39.
104. Botschaft GwG 2019, S. 5522.

Luchsinger Roland J., Kommentierung zu Art.11a GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Naef Franceso, Soft Law und Gewaltenteilung – Über die Kunst der Legiferierung durch die Katzenklappe, AJP 2015, S. 1109–1121.

Naegeli Vera, Kommentierung zu Art. 11a GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Naegeli Vera, Kommentierung zu Art. 29 GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Ordolli Stiliano, § 34 Die Schweizerische Meldestelle für Geldwäscherei und ihre Tätigkeit, in: Sester Peter/Brändli Beat/Bartholet Olivier/Schildknecht Reto (Hrsg.) Finanzmarktaufsicht und Finanzmarktinfrastrukturen: St. Galler Handbuch zum Schweizer Finanzmarktrecht, Zürich 2017.

Taube Tamara, Die Schwarze Liste der FATF – was droht der Schweiz wirklich?», recht 2014, S. 210–217.

Thelesklaf Daniel, Kommentierung zu Art. 11a GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell-Füssli-Kommentar GwG/AMLA, 3. Aufl., Zürich 2019.

Thelesklaf Daniel, Kommentierung zu Art. 23 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell-Füssli-Kommentar GwG/AMLA, 3. Aufl., Zürich 2019.

Thürer Daniel, «Soft Law» – eine neue Form von Völkerrecht?, Zeitschrift für Schweizerisches Recht (ZSR) 104 I, S. 429–453.

MATERIALIENVERZEICHNIS

Bericht der Eidgenössischen Finanzkontrolle: Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei, 20.12.2021, abrufbar unter https://www.efk.admin.ch/wpcontent/uploads/publikationen/berichte/sicherheit_und_umwelt/justiz_und_polizei/20146/20146be-endgueltige-fassung-v04.pdf, besucht am 30.11.2024 (zitiert Bericht EFK).

Botschaft zum Bundesgesetz über die Sperrung und die Rückerstattung unrechtmässig erworbener Vermögenswerte ausländischer politisch exponierter Personen vom 21.5.2014, BBl 2014 5265 ff. abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/1134/de, besucht am 30.11.2024 (zitiert Botschaft SRVG 2014).

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 30.11.2024 (zitiert Botschaft GwG 1996).

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 30.11.2024 (zitiert Botschaft GwG 2019).

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBl 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2012/1031/de, besucht am 30.11.2024 (zitiert Botschaft GwG 2012).

Botschaft zur Genehmigung und zur Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie zur Verstärkung des strafrechtlichen

Instrumentariums gegen Terrorismus und organisierte Kriminalität vom 14.9.2018, BBl 2018 6427 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2018/2301/de, besucht am 30.11.2024 (zitiert Botschaft Verhütung Terrorismus 2018).

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financère (GAFI) vom 13.12.2013, BBl 2014 605 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/100/de, besucht 30.11.2024 (zitiert Botschaft GwG 2014).

Egmont Group of Financial Intelligence Units Charter, 2013 (revised 2023), abrufbar unter https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-Charter-Revised-July-2023-Abu-Dhabi-UAE.pdf, besucht am 30.11.2024 (zitiert Egmont Charter).

Egmont Group of Financial Intelligence Units, Support and Compliance Process, 2014, abrufbar unter https://egmontgroup.org/wpcontent/uploads/2021/09/Egmont_Group_of_Financial_Intelligence_Units_Support_and_Compliance_Process.pdf, besucht am 30.11.2024 (zitiert Egmont Compliance Process).

Egmont Group of Financial Intelligence Units: Understanding FIU Operational Independence and Autonomy, Toronto (CAN) 2018, abrufbar unter https://egmontgroup.org/wp-content/uploads/2021/09/2018_Understanding_FIU_Operational_Independence_and_Autonomy.pdf, besucht am 30.11.2024 (zitiert Understanding FIU Operational Independence and Autonomy).

Egmont Group, Principles for information exchange between financial intelligence units, October 2013 (revised April 2023), abrufbar unter https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf, besucht am 30.11.2024 (zitiert Egmont Principles Exchange).

Erläuterungen zur Teilrevision der MGwV, 27.11.2019, abrufbar unter https://www.ejpd.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/vo-anpassung/erlaeuterungen-mgwv-d.pdf.download.pdf/erlaeuterungen-mgwv-d.pdf, besucht am 30.11.2024 (zitiert Erläuterungen Teilrevision MGwV 2019).

Fourth Mutual Evaluation Report on Anti-Money Laundering and counter-terrorist financing measures, Switzerland, December 2016, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/images/mer/mer-switzerland-2016.pdf, besucht am 30.11.2024 (zitiert MER 2016).

Geschäftsordnung fedpol/MROS vom 1.11.2022, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/geschaeftsordnung-mros.pdf.download.pdf/geschaeftsordnung-mros-d.pdf, besucht am 30.11.2024.

International Standards on Combating Money laundering ans the Financing of Terrorism and Proliferation – The FATF Recommendations, Paris 2012 (revised November 2023), abrufbar unter fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF Recommendations 2012.pdf.coredownload.inline.pdf, besucht am 30.11.2024 (zitiert FATF-Empfehlung[en]).

Jahresberichte der Meldestelle für Geldwäscherei (MROS), abrufbar unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 30.11.2024 (zitiert Jahresbericht MROS, jeweiliges Jahr)

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, besucht am 30.11.2024.

Third Enhanced Follow-up Report & Technical Compliance Re-Rating, January 2020, abrufbar unter https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur3-switzerland-2020.html, besucht am 30.11.2024 (zitiert FUR 2020).