Financial Intelligence Unit

ZOLL

goAML Web 2-Faktor-Authentisierung (2FA)

Das Dokument einschließlich aller seiner Teile ist urheberrechtlich geschützt. Mit Ausnahme der Nutzung ausschließlich für interne Zwecke ist jede Verwertung und Vervielfältigung ohne ausdrückliche Zustimmung der FIU Deutschland unzulässig. Dies gilt medienunabhängig insbesondere für Wiedergaben, Kopien, Mikroverfilmung, Übersetzungen sowie die Speicherung und Verarbeitung in elektronischen Systemen.

Inhaltsverzeichnis

goAML Web 2-Faktor-Authentisierung (2FA) 1

1. Allgemein 1

2. Nutzung 1

2.1. Erstmalige Einrichtung 1

2.2. Anmeldung mittels Verifizierungscode (OTP) 3

3. Sonstiges 4

© FIU Deutschland

goAML Web 2-Faktor-Authentisierung (2FA)

1. Allgemein

Die Einführung der 2-Faktor-Authentisierung am *01. September* 2025 dient der Steigerung der Sicherheit bei der Anmeldung bei goAML Web und der dort gespeicherten Daten. Es wird ein weiterer Sicherungsmechanismus implementiert und damit unbefugten Dritten der Zugriff auf die in goAML Web gespeicherten Daten weiter erschwert. Die Aktivierung gilt hierbei für alle Nutzerinnen und Nutzer von goAML Web.

2. Nutzung

goAML Web sieht derzeit nachfolgende Möglichkeit zur Nutzung als zweiten Faktor vor:

- **OTP** – One Time Password

Beim sog. OTP-Verfahren wird von goAML Web nach Eingabe Ihrer Zugangsdaten automatisiert ein Verifizierungscode generiert und an die in Ihrem Benutzerkonto hinterlegte E-Mail-Adresse gesendet. Aus Sicherheitsgründen hat der Verifizierungscode nur eine begrenzte Gültigkeitsdauer.

Den Verifizierungscode müssen Sie ferner nur einmal pro Anmeldevorgang eingeben. Eine zusätzliche Eingabe (z.B. bei Meldungsabgabe oder dem Versand einer Mailbox-Nachricht) ist nicht notwendig.

Zur Steigerung der IT-Sicherheit empfehlen wir den Empfang des Verifizierungscodes bzw. den Abruf der entsprechenden E-Mail auf einem anderen Gerät als dem zur Nutzung von goAML Web verwendeten.

Die Nutzung eines anderen zweiten Faktors wird in einer zukünftigen Version von goAML Web ermöglicht.

2.1. Erstmalige Einrichtung

Für die Nutzung des OTP-Verfahrens muss die im Benutzerkonto hinterlegte E-Mail-Adresse immer aktuell sein, sonst wird eine Nutzung des Meldeportals nicht mehr möglich sein.

Die für Ihr goAML Web Benutzerkonto aktuell hinterlegte E-Mail-Adresse können Sie nach Anmeldung bei goAML Web im Menü unter „MEIN GOAML“ und „Details zum

Benutzerkonto“ einsehen und ändern. Weiterführende Informationen zum Menüpunkt „MEIN GOAML“ bzw. dem Ändern von Daten entnehmen Sie bitte den Ausführungen des Handbuch goAML Web Portal in Abschnitt 10.

Bitte stellen Sie sicher, dass für jeden Nutzer von goAML Web in Ihrem Hause eine eigene E-Mailadresse hinterlegt ist, so dass jeder in der Lage ist, den Verifizierungscode zu erhalten.

Bitte prüfen Sie ebenso Ihre IT-Einstellungen um sicherzustellen, dass Sie bspw. E-Mails der goAML Web-Absenderadresse (bittenichtantworten@fiu.bund.de) empfangen können, ein kontinuierlicher Abruf von E-Mails innerhalb weniger Minuten gewährleistet ist und eingehende E-Mails nicht abgewiesen oder in Ihren Spam-/Junk-Ordner verschoben werden.

Den fehlerfreien Empfang von durch goAML Web versandten E-Mails können Sie zusätzlich durch Nutzung der „Passwort vergessen“-Schaltfläche auf der Anmeldemaske von goAML Web verifizieren.

Abbildung 1 – Schaltfläche zur Zurücksetzung des goAML Web Passworts

Sollten Sie nach Eingabe der dort erbetenen Daten innerhalb weniger Minuten eine E-Mail mit einem personalisierten Link zur Zurücksetzung des Passworts erhalten haben,

ist ein Empfang grds. gegeben. Die Vergabe eines neuen Passworts im Zuge dieser Prüfung ist nicht zwingend erforderlich und die empfangene E-Mail kann Ihrerseits als gegenstandslos betrachtet werden.

Eine Übersicht der Anwendungsfälle, in denen goAML Web E-Mail-Benachrichtigungen verschickt (z.B. im Rahmen der Registrierung oder bei der Übermittlung von Verdachtsmeldungen), entnehmen Sie bitte den Ausführungen des Handbuch goAML Web Portal in Abschnitt „Allgemeine Hinweise“. Sollten Sie bis dato noch keinerlei E-Mails im Rahmen der Nutzung von goAML Web erhalten haben, kann dies ein Indiz für eine fehlerhafte E-Mail-Adresse oder technische (Fehl-)Konfiguration sein (vgl. Hinweise in Abschnitt 3 dieses Schreibens).

Weitere Konfigurationen für die Nutzung des Verifizierungscodes (OTP) sind durch Sie nicht durchzuführen.

2.2. Anmeldung mittels Verifizierungscode (OTP)

Für das OTP wird nach Eingabe des Benutzernamens und des Passworts eine E-Mail mit dem Verifizierungscode an Sie übermittelt. Der sich öffnende Anmeldedialog in goAML Web zeigt ein Menüfenster zur Eingabe dieses Verifizierungscodes und die Zeit, bis zu der Sie sich anmelden müssen, bevor der OTP-Code ungültig wird.

Abbildung 2 – beispielhafte Eingabemaske bei Nutzung von OTP

Nach Eingabe des per E-Mail übermittelten Verifizierungscodes und Bestätigen der Schaltfläche „ANMELDEN>>“ werden Sie auf die bekannte Startseite von goAML Web weitergeleitet.

3. Sonstiges

Sollten Sie erst nach Aktivierung der 2-Faktor-Authentisierung feststellen, dass Ihre E-Mail-Adresse nicht mehr aktuell bzw. fehlerhaft ist und Sie somit keinen Verifizierungscode für den Login erhalten, empfehlen wir zur Korrektur eine Anfrage per E-Mail an Registrierung.gzd@fiu.bund.de.

Um Probleme mit der Übermittlung von E-Mails vorab zu vermeiden, empfehlen wir ferner Umlaute (ä, ö oder ü) nicht als Bestandteil Ihrer E-Mail-Adresse zu verwenden.

Wenn Sie eigene IT-Anwendungen nutzen, um Meldungen bei der FIU einzureichen, beachten Sie bitte, dass diese ggf. angepasst werden müssen.