DSLH HOLDING GMBH

Hohenstaufenstraße 32 · D-42287 Wuppertal · Germany
Wuppertal Local Court, Commercial Register HRB 26895

AML POLICY

Anti-Money-Laundering Policy

Anti-money-laundering and counter-terrorist-financing measures pursuant to the German GwG, FATF Standards and EU requirements

Document Version 2.0 · April 2026
Approved by: Management of DSLH Holding GmbH
Scope: all business relationships, transactions and services

1. PURPOSE AND SCOPE

1.1 Purpose

This AML Policy sets out the measures taken by DSLH Holding GmbH to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. It is based on the German Anti-Money Laundering Act (Geldwäschegesetz, GwG), the EU AML Directives (most recently the 6th AMLD and the 2024 EU AML Package) and the 40 Recommendations of the Financial Action Task Force (FATF).

1.2 Scope

This Policy applies to all business relationships, transactions and services of the Company, in particular family-office services, participations, intermediation services for larger projects, corporate finance / M&A advisory and investments.

2. LEGAL FRAMEWORK

Legal Basis	Content and Requirements
German GwG	Anti-Money Laundering Act (Geldwäschegesetz) as amended. Due-diligence, reporting, record-keeping and organisational obligations.
Section 261 StGB	Money-laundering offence in the German Criminal Code.
EU AML Directives	In particular the 5th and 6th AML Directives, the EU AML Regulation (AMLR) and the establishment of the EU AML Authority (AMLA).
BaFin Guidance	BaFin Interpretation and Application Guidance on the GwG; supervisory expectations for obliged entities.
FATF Recommendations	40 FATF Recommendations — risk-based approach, transparency on beneficial owners.
GDPR / BDSG	Processing of personal data for compliance purposes pursuant to Art. 6(1)(c) GDPR in conjunction with Section 11a GwG.
DAC8 / TFR	EU rules on reporting obligations for crypto-assets (DAC8) and the Transfer-of-Funds Regulation (TFR / Travel Rule).
HGB / GmbHG	General commercial- and corporate-law obligations.

3. RISK-BASED APPROACH

3.1 Risk Assessment

The Company performs a risk assessment for each new business relationship pursuant to Section 5 GwG. The following factors are evaluated:

- Nature and purpose of the business relationship and the service offered
- Country of origin and geographic risk of the contracting party
- Industry and business activities of the contracting party
- Ownership structure and beneficial owners (Section 3 GwG)
- PEP status (Section 1(12) GwG)
- Type, complexity and volume of the transaction

3.2 Risk Classification

Risk Class	Criteria	Measures
Low	Regulated markets, transparent ownership, no PEP status, established companies	Simplified due-diligence under Section 14 GwG, annual update

Risk Class	Criteria	Measures
Medium	Growth markets, complex structures, high transaction volumes, offshore elements	Standard due-diligence under Section 10 GwG, semi-annual monitoring, management approval
High	PEP or PEP environment, FATF / EU high-risk countries, unclear ownership, cash payments	Enhanced due-diligence under Section 15 GwG, monthly monitoring, management approval required
Unacceptable	Sanctioned persons / countries, known criminal background, anonymous transactions	Reject business relationship; report to the FIU under Section 43 GwG

4. CUSTOMER DUE-DILIGENCE OBLIGATIONS (KNOW YOUR CUSTOMER)

4.1 Simplified Due Diligence (Low Risk, Section 14 GwG)

- Identification of the contracting party using official documents
- Basic sanctions-list screening (EU, OFAC, UN, BAFA)
- Documentation of the business relationship

4.2 Standard Due Diligence (Medium Risk, Section 10 GwG)

- Full identification of natural and legal persons
- Establishment and verification of beneficial owners (Section 11 GwG); cross-check against the Transparency Register
- Understanding the purpose and nature of the business relationship
- Ongoing monitoring of the business relationship

4.3 Enhanced Due Diligence (High Risk, Section 15 GwG)

- All measures of standard due diligence
- Obtaining additional information on the source of funds
- Evidence of the source of wealth
- Management approval required before commencing the business relationship
- Increased monitoring frequency (monthly at minimum)
- Documentation of all decisions with justification

5. IDENTIFICATION AND VERIFICATION

5.1 Legal Entities

Document	Requirement
Commercial Register Extract	Current (not older than 3 months); original copy or certified extract
Articles of Association	Current version, dated and signed
Beneficial Owners	Identification of all persons with > 25% ownership or control (Section 3 GwG); Transparency Register extract
Financial Statements	Minimum of 2 financial years, audited or internal
Organisational Chart	Full ownership structure down to the natural-person level
Sanctions Screening	Screening against EU, OFAC, UN and BAFA sanctions lists

5.2 Natural Persons

Document	Requirement
Official Photo ID	Passport or identity card, valid; original review or certified copy / VideoIdent / NotarIdent

Document	Requirement
Proof of Address	Not older than 3 months (utility bill, bank statement, official letter)
PEP Check	Screening against international PEP databases
Source of Funds	For transactions > EUR 100,000: evidence of origin of funds required
Source of Wealth	For high risk: evidence of origin of wealth

6. REPORTING OBLIGATIONS

IMPORTANT: Any suspicion of money laundering or terrorist financing must be immediately reported to the German Financial Intelligence Unit (FIU) at the General Customs Directorate pursuant to Section 43 GwG. The tipping-off prohibition under Section 47 GwG must be strictly observed — the contracting party must not be informed of the report.

6.1 Internal Reporting Chain

- Employee identifies suspicious activity → immediate internal report to the AML Officer
- AML Officer reviews the matter within 24 hours
- Upon confirmed suspicion: electronic report to the FIU via the goAML portal (www.fiu.bund.de)
- In parallel: hold the affected transaction pursuant to Section 46 GwG until clarification
- Full documentation of all steps and decisions

6.2 Exceptions to Reporting

There is no reporting obligation for information covered by professional secrecy (Section 43(2) GwG), in particular within the context of legal-advice relationships.

7. TRANSACTION MONITORING

7.1 Thresholds

Threshold	Measure
EUR 10,000 (cash transactions / precious metals)	Written identification and documentation mandatory under Section 10(3) GwG
EUR 15,000 (occasional customers)	Identification of the contracting party under Section 10(3)(2) GwG
EUR 100,000 (internal)	Source-of-funds evidence required for all payment methods
Suspicious patterns	Regardless of amount: report to the FIU upon suspicion of money laundering
Crypto transactions	Full documentation under DAC8 / TFR; only regulated, MiCA-compliant providers

7.2 Red Flags — Warning Signals

- Unusually complex or incomprehensible transaction structures
- Frequent changes in ownership without economic justification
- Transactions with no apparent economic purpose
- Pressure for rapid execution without due-diligence review
- Payments to/from high-risk countries or tax havens
- Clients conducting excessive cash transactions
- Contradictory information on beneficial owners
- Transactions inconsistent with any plausible business purpose

8. CRYPTOCURRENCIES AND DIGITAL ASSETS

In accordance with MiCA, DAC8, the EU Transfer-of-Funds Regulation (Travel Rule) and the FATF guidance on virtual assets, the following rules apply:

- Exclusive use of regulated, MiCA-compliant providers (CASP) with BaFin authorisation or EU passport
- Unregulated or anonymous providers are not permitted for transactional purposes
- Every crypto transaction must be fully documented via a recognised block explorer (e.g. Etherscan)
- Full identification of all wallet addresses prior to transaction execution
- Travel Rule: for transfers > EUR 1,000, sender and recipient data must be transmitted

9. RECORD-KEEPING AND DOCUMENTATION

All AML-relevant documents are retained for at least 5 years pursuant to Section 8 GwG; in light of commercial-law requirements (Section 257 HGB) and tax-law requirements, DSLH Holding GmbH applies an extended retention period of 10 years:

- KYC records and identification documents (10 years from end of business relationship)
- Transaction records and due-diligence reports
- Internal and external reports (Suspicious Activity Reports)
- Risk assessments and decision protocols
- Training records and compliance reviews

10. TRAINING AND AWARENESS

- Induction training for all employees and external advisors at the start of employment / mandate
- Annual mandatory AML training (minimum 2 hours) pursuant to Section 6(2)(5) GwG
- Ad-hoc training upon new regulatory requirements
- Documented attendance confirmation for all training sessions

11. RESPONSIBILITIES

Function	AML Responsibility
Management	Overall responsibility; approval of the AML Policy; escalation for high-risk decisions
Managing Director / AML Officer (Dirk Meissner)	Operational AML responsibility under Section 7 GwG; receipt of internal reports; contact with the FIU and BaFin
Employees / Advisors	Compliance with the policy; identification of red flags; internal reporting
External Auditor (if appointed)	Periodic review of AML processes and documentation; for audit-required entities, in the context of the annual audit

12. FINAL PROVISIONS

This AML Policy is reviewed at least annually and updated immediately upon changes to legal requirements. Violations may result in disciplinary, civil and criminal consequences. Management is responsible for the continuous currency and effectiveness of this Policy.

DSLH Holding GmbH

DSLH Holding GmbH · Hohenstaufenstraße 32 · D-42287 Wuppertal · Germany

Wuppertal, April 2026 · Approved by Management