SWISS EDITION — AI GOVERNANCE

FRAMEWORK POLICY

for a responsible use of artificial intelligence

For [FULL LEGAL NAME OF THE FIRM]

POSITIONING

A compliance-oriented governance framework based on professional secrecy, data protection, human oversight and traceability. Its adoption constitutes neither certification nor an absolute guarantee of compliance.

PUBLICATION VERSION

Version 1.1 · 11 November 2026

Law and sources verified as November 11th 2026

ESSENTIAL DISCLAIMER & DOCUMENT STATUS

PUBLICATION DISCLAIMER — TO BE RETAINED IN THE PUBLISHED VERSION

This framework policy provides a governance structure for the responsible use of AI in Swiss legal practice. It must be adapted to [FULL LEGAL NAME OF THE FIRM], its client matters, tools, suppliers, contracts, configurations, cantons of operation and international activities. Its publication or adoption constitutes neither legal advice, certification nor a guarantee of compliance with the FADP, GDPR, EU AI Act, DORA, FINMA requirements or any other rule. Compliance depends on the facts, operational measures and evidence of those measures. Review and approval by qualified Swiss legal counsel are required before adoption or publication and following any material change in the law, systems or activities.

This AWSMTECH template is intended for adaptation, adoption and implementation by the Firm. Before publication, all fields in square brackets must be completed, irrelevant options removed and the text aligned with the contracts, configurations, registers, impact assessments, incident procedures and training actually in place. Internal deadlines, security settings and lists of approved tools must remain in separate, non-public operational documents.

Interpretation

- **"must" / "prohibited":** a minimum template requirement to be made mandatory in the firm's internal policy.
- **"under applicable law":** the rule depends, in particular, on the FADP, GDPR, professional rules, cantonal law, employment law or a sector-specific regime.
- "Firm": [FULL LEGAL NAME OF THE FIRM], [LEGAL FORM], with its registered office at [POSTCODE, TOWN/CITY, CANTON], which adopts this policy and remains subject to applicable professional and cantonal rules.
- "AI Lead": [NAME OR ROLE OF THE AI LEAD / AI COMMITTEE], responsible for coordinating approvals, the register and controls, without relieving partners or lawyers of their own duties.

CONTENTS

1. Purpose, objectives and scope	4	16. Verification and quality	11
2. Operational definitions	4	17. Intellectual property	12
3. Reference legal framework	4	18. Employment and monitoring	12
4. Responsibilities	5	19. AMLA and financial activities	12
5. Register and approval	6	20. Incidents and breaches	12
6. Classification of uses	6	21. Retention and traceability	13
7. Permitted and prohibited uses	6	22. Training and controls	13
8. Professional secrecy	7	23. EU AI Act, DORA and FINMA	14
9. Client authority, instructions and consent	8	24. Entry into force	14
10. Data protection	8	Annex A. Engagement letter	16
11. Automated decisions	9	Annex B. Approval	16
12. Impact assessment	9	Annex C. Incident matrix	17
13. Processors and contracts	10	Annex D. References	17
14. International transfers	10	AWSMTECH publication note	18
15. Security and autonomous agents	11		

PART I – FOUNDATIONS & SCOPE

1. PURPOSE, OBJECTIVES & SCOPE

This policy sets out the minimum rules governing the selection, configuration and use of artificial intelligence systems in legal practice and the administration of a Swiss law firm. It has five objectives: to protect professional secrecy and confidentiality; safeguard individuals' rights; ensure the quality of legal work; maintain identifiable human accountability; and demonstrate risk-proportionate governance through verifiable evidence.

It applies to partners, lawyers, trainee lawyers, legal professionals, employees, administrative staff, temporary staff, service providers and anyone else using an AI system on the Firm's behalf. It covers separately purchased tools, AI features integrated into existing software, application programming interfaces, local models, browser extensions, personal tools and agents capable of taking actions.

PRECEDENCE RULE

In the event of a conflict, the law, professional secrecy, client instructions, orders of an authority or court, and the applicable professional and cantonal rules take precedence over this policy.

2. OPERATIONAL DEFINITIONS

Term	Working definition
AI system	A machine-based system that, for explicit or implicit objectives, produces predictions, content, recommendations, decisions or actions influencing a physical or virtual environment.
Generative AI	A system that produces, in particular, text, code, images, sound, video, summaries or analyses from instructions and input data.
Approved tool	A system entered in the Firm's register and authorised for specified use cases, data classes, user groups and configurations.
Protected data	Information covered by professional secrecy, a confidentiality obligation, data protection, a trade secret, a protective measure, a client instruction or a procedural restriction.
Sensitive personal data	A category covered by the FADP, including health data, genetic data or biometric data identifying a person; religious, philosophical, political or trade union views; intimate life or racial/ethnic origin; social assistance measures; and administrative or criminal proceedings and sanctions.
Automated individual decision	A decision based exclusively on automated processing that produces legal effects or significantly affects the individual, according to the test under applicable law.
AI incident	An event that harms or may harm confidentiality, security, rights, legal quality, the integrity of proceedings or a contractual obligation in connection with AI.

3. REFERENCE LEGAL FRAMEWORK

Governance must be determined on a case-by-case basis. As at 11 November 2026, the use of AI in Switzerland is governed in particular by existing law, including professional rules, criminal law, data protection, contract law, employment law, intellectual property, competition, non-discrimination and procedural rules. Federal work relating to the Council of Europe Convention on AI must be monitored in a controlled legal register.

- Professional secrecy: Art. 321 of the Swiss Criminal Code, Art. 13 of the Federal Act on the Free Movement of Lawyers (Lawyers Act; LLCA), cantonal rules and contractual obligations.
- Data protection: Federal Act on Data Protection (FADP) and Data Protection Ordinance (DPO); GDPR where it applies to the processing concerned.
- Employment: Art. 328b of the Code of Obligations (CO), Art. 26 of Ordinance 3 to the Employment Act (EmpO 3), protection of personality rights, proportionality and any participation rights.
- Regulated activities: Anti-Money Laundering Act (AMLA) where the Firm's activities fall within its scope; FINMA, self-regulatory organisation (SRO), DORA or contractual requirements only where actually applicable.
- European Union: EU AI Act and other EU rules only following a documented analysis of the role, territory, system and applicable timetable.

PART II – GOVERNANCE & AUTHORISATION

4. RESPONSIBILITIES & PROFESSIONAL INDEPENDENCE

AI provides assistance; it holds no client engagement, professional responsibility or final decision-making authority. Anyone who uses, approves, communicates or files an output remains responsible for their work and must have the competence, time, access to sources and authority necessary to review it.

Role	Minimum responsibilities
Governing body / partners	Adopt the policy, allocate resources, define risk appetite, appoint those responsible and approve high-risk exceptions.
AI Lead / AI committee	Maintain the register, coordinate assessments, verify controls, monitor changes and organise training.
Data protection lead	Advise on the FADP/GDPR, DPIAs, transfers, information provided to individuals and incidents.
Partner responsible for the matter	Apply client instructions, determine contractual and professional authority, and approve sensitive uses and external communications.
Security / IT	Configure access, logging, encryption, key management, backups, integration and technical response.
User	Use only authorised tools and use cases, minimise data, verify outputs and report any incident or unfamiliar functionality.

NON DELEGATION

A supplier contract, security certification, Swiss hosting or automated opinion can never replace the Firm's legal and professional analysis.

5. AI SYSTEMS REGISTER & APPROVAL PROCEDURE

No system may process information relating to a client matter until it has been entered in the register and the corresponding use case has been authorised. Approval is limited to the version, purposes, data, users, integrations and settings assessed.

5.1 Minimum register content

- supplier, product, version or model family, internal owner and authorised users;
- purpose, use case, input data, outputs, individuals affected and risk level;
- the Firm's and supplier's legal roles, processing locations, subprocessors and remote access;
- contractual basis, assessment of professional secrecy, data protection justification and client restrictions;
- retention, training, logging, security, integrations, keys, connectors and autonomous actions;
- DPIA or other required assessment, tests, approver, date of approval, conditions, exceptions and review date;
- assessment under the EU AI Act, GDPR, AMLA, FINMA or DORA, where applicable.

5.2 Reassessment triggers

A new assessment is required whenever there is a material change in the model, supplier, purpose, data, processing location, subprocessor, terms, training policy, integration, level of autonomy or affected population, or following an incident, vulnerability or change in applicable law. If the supplier fails to respond, protected data must not be used.

6. CLASSIFICATION OF USES

Class	Decision	Examples / conditions
PROHIBIT	Stop immediately; withdraw access.	Breach of professional secrecy; unassessed personal tool; uncontrolled training; unapproved autonomous external action; discriminatory or deceptive use.
SUSPEND	No use of protected data; prompt review.	Newly activated AI feature; contractual change; unknown subprocessor; unconfirmed retention or location.
AUTHORISE SUBJECT TO CONDITIONS	Documented controls, scope and duration.	The use has demonstrated value, but requires data restrictions, enhanced review, an isolated environment or client authorisation.
AUTHORISE	Approved and monitored use.	Contract, professional secrecy, security, data protection, testing and human oversight are considered adequate for the defined scope.

7. PERMITTED, RESTRICTED & PROHIBITED USES

7.1 Generally acceptable uses — approved tools only

- dictation and transcription; initial drafting; summarisation; translation; assisted research; extraction of clauses, dates or entities; preparation of chronologies; administrative automation; training using fictitious data;

- document analysis and case preparation where the data, supplier contract and confidentiality controls match the approved scope exactly;
- generation of code, scripts or formulae after security review, testing and licence checks.

7.2 Uses requiring enhanced authorisation

- use of data covered by professional secrecy or sensitive personal data;
- uses involving recruitment, staff management, conflicts of interest, client acceptance, risk assessment, fraud, AMLA, sanctions or access to a service;
- agents capable of sending, publishing, entering into agreements, making payments, deleting, moving, changing permissions or acting in a third-party system;
- generation or alteration of images, voices or videos of identifiable individuals;
- uses that may be classified as high-risk or subject to transparency requirements under the EU AI Act.

7.3 Minimum prohibitions

- entering data relating to a client matter into a public, personal or unapproved tool;
- circumventing security settings, client restrictions, access controls or logging;
- allowing a system acting alone to provide legal advice, bind the Firm, communicate with a client, a party, a court or an authority, or perform a procedural act;
- using a citation, fact, calculation, material translation or analysis without independent verification;
- concealing AI use when an information obligation or instruction requires transparency;
- engaging in social scoring, prohibited manipulation, unlawful discrimination, general surveillance, emotion inference or staff personality profiling;
- fabricating, altering or presenting as authentic any evidence, recording, image, signature, voice or identity;
- using AI alone to determine identity, beneficial ownership, AMLA classification, whether an alert should be cleared or whether a report should be made.

PART III – PROFESSIONAL SECRECY, CLIENTS & DATA

8. PROFESSIONAL SECRECY & OUTSOURCING

MANDATORY PREREQUISITE

No information protected by professional secrecy may be made accessible to an AI supplier, hosting provider, support team, model operator or subprocessor before a written assessment under Art. 321 of the Swiss Criminal Code, Art. 13 LLCA and the applicable cantonal rules.

The assessment must determine whether access is compatible with auxiliary status and secrecy obligations, or whether specific client authorisation is necessary. It covers those who may access plaintext, support access, foreign operators, requests from authorities, training, human evaluation, logs, embeddings, caches, backups and deletion.

A processing agreement, confidentiality clause, enterprise subscription, ISO certification or Swiss data centre is not sufficient on its own. The Firm must be able to control the scope, access, subprocessing chain, changes, return and deletion of data. If professional secrecy cannot be preserved with a documented level of confidence, the use is prohibited.

8.1 Minimisation rules

- use only the strictly necessary extracts; prefer isolated environments and approved local processing;
- remove identifiers and contextual details where unnecessary; check that re-identification is not reasonably possible;

- treat pseudonymised data as personal data; simply removing a name does not constitute anonymisation;
- do not import an entire case file where the purpose can be achieved using a smaller body of documents.

9. CLIENT AUTHORITY, INSTRUCTIONS & CONSENT

Before any use affecting a client matter, the responsible partner distinguishes and documents four independent questions:

1. the justification for processing under the FADP, GDPR or another regime;
2. the contractual authority conferred by the engagement letter and client instructions;
3. the lawfulness of a service provider's access to information covered by professional secrecy;
4. the client's specific restrictions concerning tools, suppliers, countries, types of data or uses.

Consent is not a universal basis and does not remedy arrangements that are disproportionate, insufficiently secure or incompatible with professional secrecy. Where used, it must be valid for the purpose concerned, sufficiently informed and documented; the consequences of withdrawal must be managed in accordance with the law and professional obligations.

9.1 Client information and choice

The Firm informs the client where required by the nature or significance of the use, instructions, the contract, applicable law or legitimate expectations. The information proportionately covers the category of use, data concerned, safeguards, human oversight, limitations and options for restrictions. Any objection is recorded in the case file and implemented through technical controls.

9.2 Fees and transparency

AI justifies neither fictitious billing nor attributing work to someone who has not performed it. The Firm applies its fee rules, engagement terms and professional requirements, and describes AI assistance where it is materially relevant to billing or requested by the client.

10. DATA PROTECTION BY DESIGN

Any AI use involving personal data must comply with lawfulness, good faith, transparency, proportionality, purpose limitation, accuracy, security, data protection by design and by default, and the information and documentation obligations of the applicable regime.

10.1 Information to individuals

The information describes, in intelligible terms, the controller, purposes, categories of recipients and, where required, international transfers. For AI-based processing, the Firm documents and communicates, at the appropriate level, the purpose, relevant functioning, main data sources, further uses and channels for exercising rights. Data protection enquiries and requests to exercise rights should be addressed to [PUBLIC CONTACT — EMAIL, URL OR POSTAL ADDRESS].

10.2 Rights

Individuals may exercise the rights conferred on them by the law applicable to the processing concerned. Depending on the circumstances, these may include access, rectification, erasure or destruction, delivery or transfer of data, objection, restriction and human review of an automated individual decision. Their scope, conditions and exceptions are not identical under the FADP, GDPR and other regimes.

10.3 Accurate data and bias

Input data and outputs used in relation to an individual, a decision or advice are assessed for relevance, accuracy, representativeness, currency and risk of bias. Reported errors are corrected at source where possible; known limitations are communicated to those relying on the system.

11. AUTOMATED INDIVIDUAL DECISIONS

Before any use case that may influence client acceptance, a conflict of interest, recruitment, employment, fraud, a service, access, pricing or an adverse measure, the use case owner establishes:

- whether there is a decision concerning an individual rather than merely preparatory analysis;
- whether the decision is based exclusively on automated processing;
- whether it produces legal effects or significantly affects the individual;
- what information must be provided and when;
- whether the individual can express their point of view and obtain review of the decision by a natural person;
- whether a statutory exception exists and its conditions are met;
- whether the GDPR or EU AI Act imposes additional obligations.

> **INTERNAL PRINCIPLE**
>
> Unless a duly documented legal obligation requires otherwise, the Firm does not entrust AI with a final adverse decision concerning an individual. Human review must be substantive: the reviewer must understand the relevant factors, be able to challenge the output and have the authority to change it.

12. IMPACT ASSESSMENT & MANAGEMENT OF HIGH RISKS

A preliminary assessment is carried out at the planning stage. A data protection impact assessment (DPIA) is conducted where intended processing is likely to result in a high risk to personality or fundamental rights, taking into account, in particular, its nature, scope, circumstances and purpose, the use of new technologies, profiling, automated decisions, large-scale processing of sensitive data or systematic monitoring.

12.1 Mandatory procedure

1. describe the system, purpose, data, flows, individuals, suppliers and less intrusive alternatives;
2. assess the likelihood and severity of risks separately, including professional secrecy, fundamental rights, discrimination and access from abroad;
3. define technical, organisational, contractual and human measures;
4. assess residual risk and obtain approval from the controller and relevant functions;
5. if a high residual risk remains, consult the Federal Data Protection and Information Commissioner (FDPIC) or, where the statutory conditions are met, the data protection adviser;
6. review the assessment following any material change or incident.

The opinion of the FDPIC or the adviser must not be presented as certification of the system. Any use contrary to data protection principles, professional secrecy or another rule remains prohibited, even where a DPIA has been conducted.

PART IV – SUPPLIERS, TRANSFERS & SECURITY

13. PROCESSORS, CONTRACTS & SUPPLIER DUE DILIGENCE

Before approval, the Firm verifies the supplier's legal, technical and organisational capacity. Where the supplier acts as a processor, the contract must meet the requirements of Art. 9 FADP and, where applicable, Art. 28 GDPR; the label "DPA" alone is not sufficient.

13.1 Minimum clauses and evidence

- processing only on instructions and for authorised purposes; no unapproved use for the supplier's own purposes;
- confidentiality and secrecy obligations for persons authorised to access data; verifiable security measures;
- express prohibition or regulation of training, fine-tuning, human evaluation, feedback-based learning and the creation of embeddings;
- list, locations, functions and control mechanism for subprocessors; advance notice of changes;
- retention, erasure, return, backups, logs, requests from authorities and contract termination;
- assistance with rights, DPIAs, incidents, investigations, audits, litigation and professional obligations;
- notification without any contractual delay incompatible with the Firm's obligations; cooperation and preservation of evidence;
- audit rights or proportionate independent assurance; vulnerability management, continuity, portability and exit;
- rights in data, outputs, configurations and content; a challenge mechanism;
- obligation to alert the Firm if an instruction appears unlawful.

13.2 Ongoing due diligence

The Firm monitors terms, security notices, model changes, subprocessors, known incidents, performance, bias, certifications and deletion capabilities. Marketing claims are corroborated by proportionate documentation, tests or contractual safeguards.

14. DISCLOSURE OF DATA ABROAD

The Firm maps the actual locations of processing and access: data centres, support, human oversight, telemetry, logs, abuse detection, embeddings, caches, backups, disaster recovery and subprocessors. An advertised hosting region does not, by itself, prove the absence of access from abroad.

- check whether the recipient country is on the Swiss list of countries ensuring an adequate level of protection;
- if not, document a recognised safeguard, including appropriate contractual clauses, and the necessary supplementary measures;
- conduct a transfer assessment where required by law or risk, including access by authorities and available remedies;
- prioritise encryption with appropriate control of keys, minimisation, pseudonymisation and data separation;
- control onward transfers; suspend or terminate processing if protection cannot be maintained;
- use statutory derogations only exceptionally, narrowly and with documentation.

DUAL ASSESSMENT

A disclosure abroad may be compatible with the FADP while remaining incompatible with professional secrecy or client instructions. Both assessments are mandatory.

15. TECHNICAL SECURITY & AUTONOMOUS AGENTS

Measures must be proportionate to the sensitivity, volume, duration, context and autonomy of the system. At a minimum, they cover identity, access, encryption, secrets, logs, segmentation, backups, continuity, deletion, vulnerabilities, test environments and integrations.

15.1 Specific requirements for agents

- least privilege, separate technical identities, temporary permissions and limited data scope;
- isolated environment, allowlist of actions, limits, and human approval before any external or irreversible action;
- protection against prompt injection, untrusted content, exfiltration, privilege escalation and action loops;
- complete log of instructions, tools invoked, data accessed, actions, errors and approvals;
- adversarial testing, failure scenarios, stop mechanism, immediate access revocation, rollback and recovery procedure;
- default prohibition on sending messages, filing documents, incurring expenditure, signing, entering into agreements, publishing, changing permissions or deleting data without explicit human approval.

PART V – LEGAL QUALITY & SPECIAL USES

16. HUMAN OVERSIGHT, VERIFICATION & QUALITY

The intensity of review increases with risk. Review is not a matter of passively rereading plausible text: it must enable the reasoning to be reconstructed, primary sources to be checked, and omissions, bias, outdated information, jurisdictional errors, conflicts and hallucinations to be detected.

16.1 Requirements for legal work

- verify every authority, citation, date, jurisdiction, provision, calculation and material fact against a reliable, up-to-date source;
- check material translations and the terminology of the jurisdiction concerned;
- review strategy, exceptions, deadlines, conflicts, risks and consequences for the client;
- never file or transmit AI-generated material without approval by a qualified professional;
- document the review where required by risk, the client engagement, the proceedings or quality assurance;
- correct internal sources and templates where a recurring error is identified.

16.2 Courts, authorities and evidence

The Firm complies with procedural rules, court orders and duties of good faith. No generated or altered content may be presented as an authentic document or evidence of human origin. Provenance, metadata and chain of custody are preserved where authenticity is relevant.

17. INTELLECTUAL PROPERTY, PERSONALITY RIGHTS & SYNTHETIC CONTENT

- check the licences for input data, models, databases, outputs, images, code and third-party content;
- do not request reproduction of protected content beyond what the law and licences permit;
- assess risks relating to substantial similarity, trade marks, unfair competition, trade secrets and personality rights;
- clearly identify synthetic images, voices or videos where required by law, the context or the risk of deception;
- obtain the necessary authorisations before using an individual's image, voice or identity;
- retain relevant provenance information and do not remove mandatory markings or metadata.

18. EMPLOYMENT, MONITORING & HUMAN RESOURCES

Processing concerning staff must comply with Art. 328b CO, Art. 26 EmpO 3, protection of personality rights, necessity, proportionality, transparency, security and applicable participation or consultation rights. A relationship of subordination increases risk and limits the scope of purportedly freely given consent.

PROHIBITED BY DEFAULT

The following are prohibited: automated performance scoring, emotion or sentiment inference, personality profiling from communications, continuous productivity monitoring, opaque ranking and automated recommendations for disciplinary action or dismissal. An exception may be considered only after a written employment law, data protection and non-discrimination assessment, with strict measures and human decision-making.

19. AMLA, SANCTIONS & FINANCIAL ACTIVITIES

Where the Firm carries out an activity within the scope of the AMLA or is subject to SRO rules, it documents the applicable obligations and allocation of responsibilities. AI may assist with collection, comparison and sorting, but a qualified person verifies sources, resolves conflicting matches and retains the rationale.

- no autonomous determination of the identity of the contracting party or beneficial owner;
- no autonomous approval of a sanctions or politically exposed person (PEP) check, risk classification or alert;
- no autonomous decision on whether to report a suspicion;
- no automated destruction of evidence or files subject to retention requirements;
- documented testing of false positives, false negatives, bias and whether lists are up to date.

PART VI – INCIDENTS, EVIDENCE & CONDITIONAL REGIMES

20. AI INCIDENTS & PERSONAL DATA SECURITY BREACHES

Everyone must immediately report, via [INTERNAL AI INCIDENT REPORTING CHANNEL], any unauthorised transmission, erroneous output with a material impact, leak, improper access, autonomous action, discriminatory behaviour, compromise, concerning supplier change or breach of this policy. No good-faith report may be delayed for fear of a penalty.

20.1 Coordinated response

1. Contain: stop or isolate the system, revoke access and prevent the incident from spreading;
2. Preserve: retain logs, prompts, outputs, versions, decisions and evidence to a proportionate extent;
3. Assess: data, professional secrecy, individuals, client matters, suppliers, countries, actions and consequences;
4. Remedy: delete or secure, request erasure by the supplier, correct outputs and protect proceedings;
5. Decide: determine the response regarding notifications, information, client measures, the court, insurer, authorities, staff and communications;
6. Learn: analyse root causes, take corrective action and update the register, tests, DPIA, contracts and training.

20.2 Notifications

Under the FADP, the Firm notifies the FDPIC as soon as possible of a data security breach likely to result in a high risk to personality or fundamental rights. It informs the data subject where necessary for their protection or where requested by the FDPIC, subject to statutory limitations. The FADP does not impose a general Swiss 72-hour deadline.

The GDPR's 72-hour deadline applies only where Art. 33 GDPR governs the breach concerned. The Firm separately determines whether to inform the client, individuals, courts, authorities, professional bodies, insurers and contractual partners, protecting professional secrecy and also documenting decisions not to notify.

21. RETENTION, TRACEABILITY & CLIENT MATTER FILES

For each category of use, the Firm determines whether instructions, outputs, approvals, logs or assessments must form part of the client matter file. Retention is based on the purpose, evidential obligations, instructions, foreseeable litigation, professional secrecy and data protection. No single rule requires every prompt to be retained or everything to be deleted automatically.

- retain the system version and sources necessary to understand a material output;
- avoid unnecessarily duplicating protected data in logs or histories;
- apply documented retention periods and deletion holds;
- preserve confidentiality, access rights and chain of custody;
- provide for return, export and verifiable deletion when a tool is withdrawn from use.

22. TRAINING, CONTROLS & CONTINUOUS IMPROVEMENT

Access to AI systems is conditional on training appropriate to the role, risk and available features. The Firm periodically checks understanding and the effectiveness of controls, rather than relying solely on an attendance certificate.

- initial training before access to protected data, with updates following material changes;
- practical exercises covering professional secrecy, minimisation, hallucinations, bias, incidents and agents;
- quality and security testing using representative scenarios;

- proportionate usage controls that respect employment law and do not constitute general behavioural surveillance;
- an accessible route for escalation and protection for good-faith reporting;
- policy reviews at least annually and whenever triggered by an incident or a change in the law, supplier or system.

23. EU AI ACT, DORA & FINMA REQUIREMENTS

23.1 EU AI Act

The Firm does not claim to be subject to or compliant with the EU AI Act without an assessment. The register identifies any role as provider, deployer, importer or distributor; place of establishment; market and affected individuals; territorial scope; prohibited practices; AI literacy; transparency obligations; high-risk classification; responsibilities relating to general-purpose AI models; and application dates, including amendments and transitional measures.

Application dates are not fixed in the Firm's public commitments. They are maintained in a controlled legal register and checked before any launch or material change.

23.2 DORA and FINMA

DORA primarily concerns financial entities in the European Union and their management of ICT-related risks. FINMA requirements apply to the addressees and activities they specify. A law firm is not automatically subject to these regimes merely because it advises a financial-sector client.

A specific layer of controls is nevertheless activated where the Firm is itself regulated, provides a service classified as outsourcing or an ICT service, enters into contractual commitments towards a regulated entity, or handles a matter to which requirements are passed on. It then covers service classification, the subprocessing chain, audit and access rights, location, incidents, continuity, testing, exit and information required by the client or authority.

24. ENTRY INTO FORCE, EXCEPTIONS & REVIEW

Every exception must be documented in writing, limited, proportionate, supported by compensating measures, approved by the relevant functions and entered in the register. No exception may authorise a breach of professional secrecy, any law, an authority's decision or a binding client instruction.

The Firm adopts a dated version, appoints an owner, retains a record of changes and communicates the relevant rules to those concerned. The policy is reviewed at least annually and without undue delay after any material change in the law, supplier, system, risk or organisation.

24.1 Adoption record and contacts — to be completed before publication

Field to complete	Firm-specific value
Full legal name and legal form	[FULL LEGAL NAME OF THE FIRM] — [LEGAL FORM]
Registered office and contact details	[ADDRESS] — [POSTCODE, TOWN/CITY, CANTON, SWITZERLAND]
Professional scope	[CANTON(S), BAR ASSOCIATION(S) OR PROFESSIONAL AUTHORITY/AUTHORITIES]
Approving body	[PARTNERS / BOARD OF DIRECTORS / OTHER BODY]

Field to complete	Firm-specific value
Policy owner	[NAME AND ROLE]
AI Lead / AI committee	[NAME, ROLE AND INTERNAL CONTACT]
Data protection contact	[NAME OR ROLE — EMAIL — URL OR POSTAL ADDRESS]
AI incident reporting	[EMAIL / TELEPHONE / INTERNAL PORTAL]
Document lifecycle	Version [X.Y] — adopted on [DD MONTH YYYY] — effective from [DD MONTH YYYY] — next review no later than [DD MONTH YYYY]

Finalisation instruction: complete all fields in square brackets, remove unnecessary alternatives and ensure that no placeholders remain in the published version.

ANNEXES – ADOPTION TOOLS

ANNEX A – ENGAGEMENT LETTER CLAUSE (TEMPLATE TO ADAPT)

USE WITH CAUTION

This clause constitutes neither universal consent nor authorisation to disclose information covered by professional secrecy. It must be adapted to the client engagement, tools and applicable professional rules.

"The Firm may use approved artificial intelligence tools to assist with certain tasks, including research, analysis, summarisation, translation and drafting. These tools do not undertake any client engagement, and their outputs are subject to human review proportionate to the risk. The Firm remains responsible for its services.

Before processing information relating to the client engagement, the Firm assesses professional secrecy, data protection, security, suppliers and subprocessors, processing locations and terms of use. It limits the data to what is necessary and does not permit protected information to be used to train shared models without a documented legal basis, authorisation and specific safeguards.

Where required by law, the nature of the engagement or your instructions, the Firm informs you of the intended use and obtains the necessary instructions or authorisations. You may specify restrictions; the Firm will advise you if these affect the manner, timing or cost of carrying out the engagement."

ANNEX B – DECISION TO APPROVE AN AI SYSTEM

Area	Decision questions
Use case	Exact purpose? Benefit? Less intrusive alternative? Users? Individuals affected? Autonomous action?
Professional secrecy	Plaintext access possible? Auxiliary status? Staff/support? Foreign law? Client authorisation? Cantonal rules?
Data	Categories, sensitivity, volume, minimisation, pseudonymisation, retention, rights, automated decision, DPIA?
Supplier	Instructions only? Training? Subprocessors? Audit? Incidents? Deletion? Portability? Financial stability?
Transfers	Countries, remote access, adequacy, clauses, transfer assessment, encryption, keys, onward transfers?
Security	Identities, MFA, roles, segmentation, logs, secrets, integrations, vulnerabilities, backups, stop, rollback?
Quality	Sources, tests, error rates, bias, limitations, human review, documentation and suspension criteria?
Regimes	FADP, GDPR, EU AI Act, AMLA/SRO, FINMA, DORA, client contracts, procedure and intellectual property?
Decision	Prohibit / suspend / authorise subject to conditions / authorise; approver, date, limits, exceptions, evidence, review.

ANNEX C — INCIDENT DECISION MATRIX

Question	Decision to document
Professional secrecy	Client engagement; information; recipient; recovery/deletion; client, court or authority to inform; protective measures.
FADP	Security breach? Is high risk likely? Notify the FDPIC as soon as possible? Inform individuals where necessary for their protection or requested by the FDPIC?
GDPR	Does the regime apply? Risk to rights and freedoms? Notify the authority within 72 hours if Art. 33 applies? Inform individuals if high risk, subject to exceptions?
Contracts / sectors	Contractual deadlines and recipients; insurer; SRO; FINMA/DORA requirements or regulated client; evidence preservation.
Quality / procedure	Has an erroneous output been used? Correction; withdrawal; information; procedural deadline; disclosure to the court; preservation of evidence.
Remediation	Cause and scope; blocking; corrective measures; tests; updates to the DPIA, register, contract and training; decision to resume operation.

ANNEX D — MAIN OFFICIAL REFERENCES

Non-exhaustive selection. Consolidated texts, cantonal rules and obligations specific to each client engagement must be checked at the time of use. Links consulted or verified for this edition on 11 November 2026.

Source	Official link
Federal Act on Data Protection (FADP), SR 235.1	Open source
Data Protection Ordinance (DPO), SR 235.11	Open source
FDPIC — AI and data protection	Open source
FDPIC — DPIA factsheet, Arts. 22 and 23 FADP	Open source
Swiss Criminal Code, Art. 321, SR 311.0	Open source
Federal Act on the Free Movement of Lawyers (Lawyers Act; LLCA), Art. 13, SR 935.61	Open source
Code of Obligations, in particular Art. 328b, SR 220	Open source
Ordinance 3 to the Employment Act, Art. 26, SR 822.113	Open source
FINMA — Self-regulatory organisations and AMLA obligations	Open source
Federal Office of Justice — Artificial intelligence	Open source
Regulation (EU) 2024/1689 on artificial intelligence, official text	Open source
Regulation (EU) 2026/1744 amending the AI Act	Open source

Source	Official link
Regulation (EU) 2016/679 (GDPR)	Open source
Regulation (EU) 2022/2554 (DORA)	Open source

AWSMTECH PUBLICATION NOTE

FINAL PUBLICATION DISCLAIMER

This framework policy may serve as a basis for publication only after all fields in square brackets have been completed and its suitability for the Firm's specific circumstances has been validated. It constitutes neither legal advice, certification nor a guarantee of compliance. Its adoption does not relieve (FULL LEGAL NAME OF THE FIRM) of the obligation to verify and demonstrate, for every use, lawfulness, professional secrecy, security, contracts, settings, human oversight and compliance with applicable cantonal or sector-specific rules. Review by qualified Swiss legal counsel is required before publication and following any material change.

For adoption by a law firm, AWSMTECH recommends maintaining separately: the AI systems register; the list of approved tools and use cases; professional secrecy assessments; DPIAs and transfer assessments; supplier assessments; technical configurations; tests; exceptions; training records; and incident files.

Responsible technology. Legal practice under control.

Framework policy — Swiss edition in English | Version 1.1 | 11 November 2026