Partnerships & Disclosure

1. Partner Due Diligence & Vetting SOP
2. Partner Disclosure Policy

Approved by: National Board

Updated: 2026-03-01

Review cycle: Annual (or earlier if legislation or practice changes)

Chapter 1. Partner Due Diligence & Vetting SOP

Policy owner: Executive Director / Procurement Lead & Ethics & Compliance Officer (ECO) (with Data Protection Officer, DPO; Designated Safeguarding Lead, DSL/CPO; Finance Manager/Chief Accountant, FM/CA)

Related policies: Procurement & Ethical Purchasing; Financial Policy; Fraud Response Plan; Whistleblowing & Complaints; Code of Conduct; Conflict of Interest (COI); GDPR & Data Protection; Privacy Policy; Data Breach Response Plan; Records Retention & Destruction; IT & Cybersecurity; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI; Media, Storytelling & Image Consent; Infiltration & Internal Surveillance Policy; Sustainability Guidelines; Business Continuity & Physical Security Standards.

---

1) Purpose & Scope

This SOP defines how we assess, approve, and monitor partners and vendors (collectively Partners) to prevent fraud, corruption, SEA/child abuse, human-rights abuses, sanctions violations, data/privacy breaches, conflict of interest, infiltration risks, and other harms. It applies to all programmatic implementing partners, sub-grantees, vendors, consultants, fiscal sponsors, and strategic collaborators prior to engagement and throughout the relationship.

2) Principles

- **Risk-based & proportionate:** checks scale with **Tier** (Low/Medium/High).
- **Legality & human rights:** align with Lithuanian/EU law, GDPR, and international norms.
- **Do No Harm & Safeguarding:** protect beneficiaries, activists, and staff.
- **Non-discrimination:** decisions based on behaviour and risk, **not** on protected characteristics.
- **Privacy-by-design:** minimise data, transparent notices (Annex O), secure handling, and defined retention.
- **Accountability & documentation:** every step recorded in the **Partner File** and **Screening Log**.
- **Independence & COI control:** declare and manage conflicts; recuse when needed.
- **Continuous monitoring:** not a one-off—re-screen and review performance.

---

3) Definitions (Plain Language)

- **Partner:** any external entity we contract with or collaborate with (implementing partner, vendor, consultant, fiscal agent, venue, media contractor).
- **Due diligence (DD):** verification of identity, capacity, integrity, compliance, and risk.
- **UBO:** Ultimate Beneficial Owner(s) who ultimately own/control an entity.
- **PEP:** Politically Exposed Person (and close associates).
- **Sanctions lists:** EU, UN, UK, US (and other relevant) restrictive measures.

- **Adverse media:** credible reports of fraud, corruption, GBV/SEA, human-rights abuses, organised crime, or extremism.
- **Tier:** risk level (Low/Medium/High) determining depth of checks and approvals.
- **Processor:** vendor processing personal data on our behalf (GDPR Article 28).

---

4) Roles & Responsibilities

- **National Board:** oversight of high-risk approvals and debarments; receives annual DD report.
- **Executive Director (ED):** final approver on **High** tier and exceptions; authorises debarment.
- **ECO (SOP owner):** maintains methodology, logs, training; triages concerns; non-retaliation.
- **Procurement Lead:** runs sourcing, obtains documents, screens vendors, files records.
- **FM/CA:** financial capacity checks; bank verification; payment holds; audit trail.
- **DPO:** privacy/GDPR checks; DPAs; transfer mechanisms; incident history.
- **DSL/CPO & PSEA Focal Point:** safeguarding/SEA checks, survivor-centred measures.
- **IT & Security Lead:** information-security controls for SaaS/tools; access risk.
- **Programme Lead/Requestor:** defines scope; validates references; monitors performance.
- **All staff:** declare COIs and report red flags.

Designated contacts (to fill): ECO; Procurement Lead; FM/CA; DPO; DSL/CPO; IT Lead; **due diligence inbox:** *partners@adliga.fund*.

---

5) Process Overview (Flow)

1. **Intake & Initiation** → Partner/Vendor Request Form (Annex A) by Programme/Requestor.
2. **Pre-Tiering** → quick risk screen (Annex G) to assign **Tier** (Low/Medium/High).
3. **Document Pack** → DD Questionnaire & Self-Declarations (Annex A/B/C/D/E).
4. **Screening** → legal, sanctions/PEP, adverse media, safeguarding/SEA, modern slavery, DEI, data protection/security, financial capacity, bank verification, references, site visit (as needed).
5. **Risk Scoring** → apply matrix (Annex H) and compile **DD Report** (Annex M).
6. **Decision & Approvals** → per **Delegation of Authority** (Annex K).
7. **Onboarding & Contracting** → clauses/checklist (Annex L), induction, KPIs.
8. **Monitoring & Re-assessment** → cadence per Tier; event-driven checks.
9. **Closure/Debarment** → if issues arise; record in Debarment Register.

---

6) Risk Tiering (Assign Before Deep Checks)

Inputs: contract value & duration; data sensitivity (GDPR); contact with children/vulnerable groups; geography & sector; criticality to operations; prior performance; payment method (cashless preferred); infiltration/context risk.

- **Tier LOW** — low value/one-off; no sensitive data; no vulnerable groups; established vendor.
- **Tier MEDIUM** — recurring spend; limited data; indirect contact with vulnerable groups.
- **Tier HIGH** — high value/strategic; handles personal data as **processor**; direct work with children/beneficiaries; high-risk geography/sector; new or opaque ownership.

Depth of Checks: see **Annex G** (matrix). **Triggers** for **DPO** (processors/transfers) and **DSL/PSEA** (child/SEA exposure).

7) Screening Checks (What to Verify)

7.1 Legal Identity & Structure

- Registration certificate, tax ID, address; statutes; **UBO** and governance list (Board/Directors).
- Litigation/insolvency search where feasible; required licences/permits.

7.2 Sanctions, PEP & Adverse Media

- Screen entity, UBOs, directors, and key signatories against **EU/UN/UK/US** lists; record results in **Screening Log** (Annex F).
- Adverse media review for corruption, **SEA/GBV**, trafficking/modern slavery, human-rights abuses, extremism.
- Document **false positive** resolution; retain evidence (screenshots/refs).

7.3 Safeguarding, Child Protection & PSEA

- Verify existence and adequacy of **Safeguarding**, **Child Protection**, and **PSEA** policies; training records; reporting mechanisms; background check practices for their staff; two-adult rule; incident history and response.

7.4 Human Rights, DEI & Non-Discrimination

- Policy commitments; grievance mechanisms; evidence of inclusive practice; no tolerance for hate speech/hate symbols; alignment with our **NDEI/DEI** standards.

7.5 Anti-Corruption, Conflicts of Interest & Ethics

- **COI Declarations** (Annex B) from both sides; anti-bribery/benefits policy; gifts & hospitality controls; whistleblowing mechanisms; past investigations or debarments.

7.6 Financial Capacity & Stability

- Audited financials (last 2 years) or management accounts; cash-flow capacity; going-concern statement; funding concentration; references from donors/clients.

- If sub-grantee: grant management capacity; segregation of duties; procurement procedures.

7.7 Bank Account & AML/KYC

- Beneficiary name matches account; IBAN/SWIFT verification; independent call-back to an official number; watch for last-minute changes; no payments to personal accounts except justified micro-grants with controls (Annex E).

7.8 Data Protection & Information Security (if Processor or Data Access)

- GDPR readiness; **DPA** terms; data location and transfer mechanisms; breach history; access controls; encryption; backups; **incident notice SLA**; sub-processors list (Annex D).
- Align with **IT & Cybersecurity Policy** and **Data Breach Response Plan**.

7.9 Health, Safety & Environment

- H&S policy; insurance (public liability where relevant); environmental commitments; waste/disposal practices; **Sustainable Procurement Scorecard** (Annex C).

7.10 Technical Capacity & References

- Staff qualifications; prior similar work; deliverables/KPIs; **site visit report** if applicable (Annex I).
- At least **two references** checked and logged.

7.11 Media & Consent Practices (where relevant)

- Alignment with **Media, Storytelling & Image Consent Policy**; consent workflows; anonymisation for at-risk groups.

7.12 Infiltration/Integrity Risk

- Per Infiltration & Internal Surveillance Policy: check for red flags; shadow groups; unusual info requests; undisclosed affiliations.

---

8) Risk Scoring & Decision

Apply the **Risk Scoring Matrix** (Annex H) across categories (Governance/Ownership;

Sanctions/PEP; Safeguarding/PSEA; Corruption/COI; Financial; Data Protection; H&S/Environment; Capacity; Context/Geography).

Thresholds (example):

- **0–14 Low** → Programme Lead + Procurement approve
- **15–29 Medium** → add ECO + FM/CA approval
- **≥30 High** → ED approval; conditions or CAP (Annex J) required
- **No-Go** criteria: listed sanctions; unresolved SEA/child abuse substantiation; known human-rights atrocities; deliberate fraud.

Document decision, conditions, and **review date** in the **DD Report**.

---

9) Onboarding & Contracting

- Use **contract clause checklist** (Annex L): Code of Conduct; **Safeguarding/Child Protection/PSEA**; anti-corruption; **GDPR/DPA**; IP/consent; audit and access rights; incident notice (breach, SEA, fraud) **within 24–72h**; sanctions/termination; sustainability clauses.
- Create **Partner File** (digital) with all forms, approvals, and screening evidence; register in Vendor/Processor and ROPA (if processor).
- Provide induction on our policies and reporting channels; agree **KPIs** and monitoring plan.

---

10) Monitoring, Re-Screening & Changes

- **Low:** re-screen **annually**; performance review at close.
- **Medium:** re-screen **annually** + event-driven; light spot checks.
- **High:** sanctions/adverse media watch **quarterly**; site/audit as needed.

Event-driven triggers: leadership/ownership change; incident/complaint; bank change; scope change; context/geography risk change; media allegations. Update risk score and approvals if Tier moves up.

11) Incidents, Escalation & Remedies

- **Immediate suspension** may apply where safety or compliance risks are high.
- Route allegations via: **Fraud Response Plan**, **SEA/Child Protection** procedures, **Data Breach** plan, and **Whistleblowing**.
- Investigate fairly; preserve evidence; coordinate with authorities when required.
- Remedies: CAP with deadlines; withhold payments; partial/total termination; recovery of funds; **debarment**.

---

12) Exceptions & Emergency Engagements

- In urgent humanitarian or continuity needs, a **time-bound exception** may be granted by ED (Annex Q) with ECO/Procurement advice and compensating controls (e.g., payment caps, enhanced monitoring). Complete full DD **within 30 days**.

---

13) Debarment & Blacklisting

- Grounds: sanctions; substantiated SEA/child abuse; fraud/corruption; repeated severe breaches; refusal to cooperate.
- **Process:** ECO drafts case; ED decides; notify partner; record in **Debarment Register**; communicate internally; review after minimum **24 months** if remediation evidence exists.

---

14) Records, Privacy & Retention

- Maintain DD records in secure DMS with role-based access; encrypt sensitive files.
- **Retention: 10 years after relationship end** (or longer if law/donor requires).
- Provide **GDPR notices** to partner contacts (Annex O); only collect necessary personal data; limit sharing to approval chain; log access.

- Cross-reference **Records Retention & Destruction Schedule**.

---

15) Training & Awareness

- Induction for staff involved in sourcing, grants, and partnerships.
- **Annual refreshers** on screening tools, red flags, safeguarding, GDPR, and infiltration risks.
- Refresher briefings when thresholds/matrices change.

---

16) Review & Continuous Improvement

- ECO/Procurement review KPIs and case studies **annually**; update forms and thresholds; report to National Board.
- Conduct **spot audits** of Partner Files and Screening Logs.

Annexes (Forms, Logs & Checklists)

Annex A — Partner/Vendor Information & Self-Declaration

- Legal details; UBOs; contacts; scope; policies; certifications; prior incidents; acceptance of our Code of Conduct.

Annex B — Conflict of Interest (COI) Declarations

- For Organization staff involved and Partner signatories; mitigation/recusal plan.

Annex C — Safeguarding/Child Protection & PSEA Questionnaire

- Policies, training, reporting, vetting, incident handling, survivor-centred approach.

Annex D — Data Protection & Security Questionnaire (+DPA checklist)

- Lawful bases; categories; transfers; sub-processors; TOMs; breach notice SLA; DPIA flag; ROPA entry.

Annex E — AML/KYC & Bank Details Verification Form

- IBAN/SWIFT; beneficiary verification; call-back script; change-request controls.

Annex F — Sanctions/PEP/Adverse Media Screening Log

- Names searched; lists/providers; date; result; analyst; evidence ref; false positive notes; re-screen date.

Annex G — Tiering Tool (Risk-Based Checklist)

- Value; data; vulnerable groups; geography; sector; criticality; ownership opacity; prior performance; outcome = Low/Medium/High.

Annex H — Risk Scoring Matrix

- Weighted categories and thresholds; go/no-go rules.

Annex I — Site Visit / Remote Assessment Report

- Facility; interviews; controls; photos (non-sensitive); gaps; recommendations.

Annex J — Corrective Action Plan (CAP) Template

- Findings; actions; owner; deadline; evidence; verification; status.

Annex K — Approval & Delegation of Authority Matrix

- Who approves which tier/value; quorum; substitutes; signature blocks.

Annex L — Contract Clause Checklist

- Code of Conduct; Safeguarding/SEA/Child Protection; Anti-corruption; GDPR/DPA; IP/Consent; Audit; Incident Notice; Sanctions/Termination; Sustainability; Supplier Code of Conduct.

Annex M — Due Diligence Report Template

- Summary; tier and score; key findings; decision; conditions; review date.

Annex N — Debarment Notice Template

- Grounds; effect; appeal/review terms; internal distribution list.

Annex O — Privacy Notice for Partner Due Diligence (GDPR Art. 13/14)

- Controller; purposes; legal bases; recipients; transfers; retention; rights; contact.

Annex P — Ongoing Monitoring Plan

- KPIs; reporting cadence; audit/site visit schedule; triggers; responsible owners.

Annex Q — Emergency Exception & Risk Acceptance Form

- Justification; duration; compensating controls; ED approval; follow-up DD due date.

Chapter 2. Partner Disclosure Policy

Related policies: Partner Due Diligence & Vetting SOP; Procurement & Ethical Purchasing Policy; Code of Conduct; Conflict of Interest (COI) Policy; Whistleblowing & Complaints Policy; GDPR & Data Protection Policy; Privacy Policy; IT & Cybersecurity Policy; Data Breach Response Plan; Records Retention & Destruction Schedule; Child Protection & Safeguarding Policy; SEA Prevention & Response Policy; Financial Policy; Fraud Response Plan; Media, Storytelling & Image Consent Policy; Infiltration & Internal Surveillance Policy; Sustainability Guidelines.

---

1) Policy Statement & Purpose

This Policy sets mandatory disclosure and notification obligations for all Partners (vendors, consultants, implementing partners, sub-grantees, fiscal sponsors, strategic collaborators) to ensure the Organization can assess risk, meet legal duties, protect beneficiaries, and uphold integrity throughout the relationship. It complements the Partner Due Diligence & Vetting SOP by specifying what must be disclosed, when, and how, including ongoing changes and incidents.

Objectives: (a) ensure transparency on ownership, capability, compliance, and risks; (b) detect and mitigate issues early; (c) protect people and data; (d) support fair, lawful, non-discriminatory decision-making; (e) document accountability.

---

2) Scope & Applicability

Applies to all Partners engaged by the Organization at any value/term, and to their subcontractors, agents, and sub-processors involved in delivering contracted services. Disclosure obligations apply pre-engagement, during contracting, and throughout the partnership until all obligations are fulfilled and records closed.

---

3) Definitions (Plain Language)

- **Partner:** any external entity we contract with or collaborate with, including implementing partners, sub-grantees, consultants, vendors, venues, media contractors, fiscal agents.
- **Material change:** any change reasonably likely to affect risk or our ability to meet legal/contractual duties (e.g., ownership, leadership, financial solvency, sanctions status, incidents, data handling, staffing for sensitive roles).
- **Incident:** a significant event involving harm, breach of law/policy, or risk to people or data (e.g., **safeguarding/SEA**, data breach, fraud, corruption, discrimination/harassment, H&S, environmental spill).
- **Sub-processor:** any third party a Partner uses to process personal data for our purposes.
- **UBO:** ultimate beneficial owner(s) who ultimately own/control the Partner.

---

4) Principles

1. **Legality & human rights:** disclosures support compliance with Lithuanian/EU law, GDPR, and international norms.
2. **Do No Harm & safeguarding:** prioritise safety of beneficiaries and staff; survivor-centred approach.
3. **Non-discrimination:** risk-based, behaviour-based decisions—**never** on protected characteristics.
4. **Privacy-by-design:** minimise personal data in disclosures; provide privacy notices; secure storage and defined retention.

5. **Accuracy & timeliness:** complete, truthful, and prompt disclosures; corrections supplied without delay.
6. **Accountability:** documented attestations; audit rights; consequences for misrepresentation.

---

5) Required Disclosures (Pre-Engagement & Annual Attestation)

Partners must provide accurate information and supporting documents, including where applicable:

- **Legal identity & governance:** registration, tax ID, address, statutes; list of directors/Board; **UBO declaration**.
- **Sanctions/PEP/adverse media:** confirmation of screening for entity, UBOs, and key officers; disclosure of any listings, investigations, or relevant adverse media.
- **Safeguarding/Child Protection/SEA:** policies, training, reporting channels; **two-adult rule**; incident history and outcomes; pending investigations.
- **Human rights, DEI & non-discrimination:** policies and grievance mechanisms; any substantiated violations.
- **Anti-corruption & COI:** anti-bribery policy; **Conflict of Interest declarations** from Partner signatories; gifts & hospitality rules; past debarments.
- **Financial capacity & stability:** audited accounts (2 years) or management accounts; going-concern statement; key funding sources.
- **Banking & AML/KYC:** verified bank details matching legal beneficiary; change-control process; confirmation of AML controls.
- **Data protection & security (if processing personal data or accessing systems):** data categories, purposes, locations, **sub-processor list**, security measures, breach history, **DPA** readiness, international transfer mechanisms (e.g., SCC/DPF).
- **Health, safety & environment:** H&S policy, insurance (as relevant), environmental commitments.
- **Technical capacity & staffing:** key personnel qualifications/background checks where role-appropriate.

- **Subcontractors/agents:** list and roles; due-diligence approach; contract flow-down clauses.
- **Media & consent practices (if applicable):** alignment with our Media/Consent Policy; anonymisation options for at-risk groups.
- **Litigation/regulatory:** any current or recent (last 5 years) material litigation, regulatory actions, or licence issues.
- **Other material facts:** any information a reasonable person would consider relevant to risk and performance.

Partners must **renew** these disclosures via an **Annual Partner Attestation** and upon request.

---

6) Ongoing Notifications (Change & Incident Triggers)

Partners must notify the Organization in writing at **partners@adliga.fund** (or as specified in contract) within:

- **24 hours** — suspected/actual **safeguarding/SEA incidents**; **personal data breaches**; serious **fraud/corruption** allegations; **criminal conduct** on the engagement.
- **72 hours** — major **IT/security incidents** without personal data; serious **H&S/environmental** incidents.
- **5 business days — material changes**: ownership/UBO/leadership; sanctions/PEP status; subcontractors/sub-processors; location of data processing; scope of services; bank account changes; start of significant litigation/regulatory investigations; staffing of sensitive roles; dissolution/insolvency risk.

Notifications must include available facts, interim controls, and a contact person; updates follow as new facts emerge.

---

7) Process & Responsibilities

- **Partner:** submit disclosures using the **Partner Disclosure Form** (Annex A) and attach evidence; maintain records; provide timely updates; cooperate in reviews and audits.

- **Procurement Lead/ECO:** receive and log disclosures; coordinate reviews with DPO/DSL/FM/IT; request clarifications; record decisions and conditions.
- **DPO:** review privacy/security disclosures and DPAs; advise on DPIA/TIA and breach notifications.
- **DSL/CPO & PSEA Focal Point:** review safeguarding/SEA aspects and incident responses.
- **FM/CA:** review financial capacity and bank verification.
- **ED:** approve high-risk cases/exceptions; decide on suspensions/terminations.

All disclosures are stored in the **Partner File** and **Screening/Disclosure Log** with role-based access.

---

8) Verification, Audit & Site Visits

The Organization may **verify** disclosed information through references, public registers, third-party screening, and **site or remote assessments**. Partners must provide reasonable access to relevant records and people. Audit rights are exercised **proportionately** and with notice, as set in the contract.

---

9) Privacy, Confidentiality & Use of Disclosures

We collect only data necessary to assess and manage the partnership, process them under a lawful basis (contract/legal obligation/legitimate interests), and store them securely per our GDPR & Data Protection and Records Retention policies. We use disclosures solely for risk assessment, compliance, and contract management; sharing is limited to authorised personnel and regulators as required by law.

Partners receive a Privacy Notice for Due Diligence (Annex F).

---

10) Decisions, Conditions & Corrective Actions

Outcomes may include approval, approval with conditions/Corrective Action Plan (CAP), deferral pending evidence, or rejection/termination. Conditions

may cover training, policy adoption, DPAs, staffing changes, sub-processor restrictions, enhanced reporting, or audits. Decisions and rationales are documented in the Disclosure Review Record (Annex D).

---

11) Non-Compliance, Misrepresentation & Remedies

Failure to disclose, late notification, or false/misleading statements may result in: hold on payments; suspension; contract variation; recovery of funds; termination for cause; debarment from future work; and reporting to authorities/donors where required. The Organization will apply remedies fairly and proportionately.

---

12) Records & Retention

Maintain disclosure records for 10 years after relationship end (or longer if law/donor requires). Keep a Change & Incident Log linked to each Partner File. See the Records Retention & Destruction Schedule.

---

13) Training & Communication

We provide Partners with onboarding materials, policy links, and reporting channels. Internal staff involved in partnerships receive induction and **annual refreshers** on disclosure requirements and review procedures.

---

14) Review & Continuous Improvement

The ECO/Procurement Lead reviews this Policy annually or after significant legal/operational changes and reports to the National Board. Lessons learned from cases feed into updates to thresholds, templates, and contracts.

Annexes (Forms & Logs)

Annex A — Partner Disclosure Form (Initial/Annual)

- Identity/governance/UBO; sanctions/PEP/adverse media; safeguarding/SEA; DEI/human rights; anti-corruption/COI; financials; AML/KYC; data protection & security; H&S/environment;

subcontractors/sub-processors; litigation/regulatory; media consent practices; other material facts; attestation.

Annex B — Conflict of Interest Declaration (Partner)

- Parties; relationship; risk; mitigation/recusal plan; signature.

Annex C — Beneficial Ownership & Control Declaration

- UBO names/percentages; control structures; changes since last attestation.

Annex D — Disclosure Review Record

- Reviewer(s); date; findings; conditions/CAP; decision; next review date.

Annex E — Change & Incident Notification Form

- Trigger type; date/time; facts; interim controls; requested action; attachments; follow-up schedule.

Annex F — Privacy Notice for Partner Due Diligence (Art. 13/14 GDPR)

- Controller; purposes; lawful bases; recipients; transfers; retention; rights; contact.

Annex G — Annual Partner Attestation

- Statement of completeness/accuracy; list of changes since last attestation; signature; date.