

Ethics & Integrity

1. **Code of Conduct**
2. **Whistleblowing & Complaints**
3. **Conflict of Interest**
4. **Infiltration & Internal Surveillance Policy**

Approved by: National Board

Updated: 2026-03-01

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

Chapter 1. Code of Conduct

Related policies: Child Protection & Safeguarding Policy; Sexual Exploitation & Abuse (SEA) Prevention & Response Policy; Data Protection/Privacy Policy; Whistleblowing & Complaints Procedure; Anti-Harassment Policy; Partner & Vendor Due Diligence Standards.

1) Policy Statement & Purpose

This Code sets the ethical and professional standards expected of all who represent the Organization. It promotes a culture of integrity, respect, accountability, transparency, and inclusion, and protects our reputation and the communities we serve.

Objectives: (a) prevent misconduct and conflicts of interest; (b) define acceptable behaviour online/offline; (c) ensure non-discrimination and safety; (d) provide reporting channels and consequences for violations.

2) Scope and Applicability

Applies to all personnel and associated parties: employees (permanent/temporary), volunteers, interns, National Board members, consultants, contractors, suppliers, visitors, and implementing partners when acting for or on behalf of the Organization.

Condition of engagement: Compliance with this Code is mandatory. Breaches may trigger disciplinary action up to termination and/or referral to authorities.

3) Definitions (Plain Language)

- **Conflict of interest (COI):** a situation where personal interests (financial, familial, political, or other) could improperly influence professional judgment.
 - **Harassment:** unwanted conduct (verbal, non-verbal, physical) that has the purpose or effect of violating dignity or creating a hostile, intimidating, degrading, humiliating, or offensive environment.
 - **Bullying:** repeated unreasonable behaviour that creates risk to health/safety.
 - **Discrimination:** unfair treatment based on protected characteristics (e.g., sex, gender identity, age, disability, race/ethnicity, nationality, religion/belief, sexual orientation).
 - **Fraud & corruption:** deception for personal/organizational gain; bribery, embezzlement, kickbacks.
 - **Gifts & hospitality:** anything of value offered/received (goods, services, travel, entertainment).
 - **Safeguarding/SEA:** as defined in our related policies (child protection; PSEA) and incorporated by reference.
-

4) Roles & Responsibilities

- **National Board:** Approves and oversees the Code; receives annual ethics/safeguarding reports and serious incident notifications.
- **Executive Director:** Ensures implementation, training, and culture; appoints focal points; applies sanctions where warranted.
- **Ethics & Compliance Officer (ECO):** Primary contact for Code violations and COI disclosures; maintains the **Ethics Register**; coordinates investigations with HR/Legal; ensures non-retaliation.

- **Designated Safeguarding Lead (DSL)/Child Protection Officer (CPO) and PSEA Focal Point:** handle safeguarding/SEA concerns under related policies; coordinate with ECO where issues overlap.
- **Managers:** Model expected behaviour; ensure team induction and adherence; address concerns promptly.
- **All personnel & associated parties:** Know and follow the Code; complete training; declare COIs; report concerns immediately.

Designated Contacts (to fill):

- **Ethics & Compliance Officer (ECO):** *Name, role, phone, email*
 - **DSL/CPO:** *Name, role, phone, email*
 - **PSEA Focal Point:** *Name, role, phone, email*
 - **Deputy (DSL/PSEA/ECO):** *Name, role, phone, email*
 - **Board Safeguarding Focal Point:** *Name, email*
-

5) Standards of Behaviour (What is Expected)

5.1 Integrity, Transparency & Accountability

- Act honestly and fairly; keep accurate records; cooperate with audits.
- **No fraud, bribery, or kickbacks.** Report solicitations of bribes immediately.
- Use organizational resources (funds, assets, vehicles, IT) **only for legitimate purposes**; prevent waste and misuse.

5.2 Respect, Inclusion & Non-Discrimination

- Treat everyone with dignity and respect; no harassment, bullying, or hate speech.
- Foster inclusive, accessible participation; make reasonable accommodations for disability and language.

5.3 Conflicts of Interest (COI)

- **Disclose** any actual, potential, or perceived COI **in writing** to the ECO using **Annex B - COI Disclosure**.

- Do not participate in decisions where COI exists until managed/approved.
- Family/close relationships in hiring, supervision, or procurement require prior disclosure and mitigation.

5.4 Gifts & Hospitality

- **Thresholds:** Accepting gifts/hospitality **over €50 per item or €100 total per year per source** requires prior written approval and entry in the **Gifts & Hospitality Register** (Annex C).
- **Prohibited:** cash or cash equivalents; gifts during tenders/procurement; anything that could influence or appear to influence decisions.
- When in doubt, **decline** and notify the ECO.

5.5 Safeguarding & PSEA (Zero Tolerance)

- Maintain professional boundaries; never exploit power imbalances.
- **Prohibited:** sexual activity with anyone under 18; **transactional sex;** sexual relationships with beneficiaries/participants; sexualised communication; possession of pornography on organizational systems/premises.
- Follow the Child Protection and SEA Policies and **report concerns immediately** to DSL/CPO or PSEA FP.

5.6 Confidentiality & Data Protection (GDPR)

- Access, process, and share personal data **only** as necessary and lawful; protect confidential information of beneficiaries, partners, donors, and staff.
- Use organizational devices/platforms; follow encryption and retention rules; report data breaches **without delay** per the Privacy Policy.

5.7 Digital Conduct & Communications

- Be professional online; no hate speech, discrimination, or shaming content.
- Do not “friend/follow” beneficiaries/children from personal accounts; use official channels.

- Obtain consent for images/stories per media policies; avoid identifying details of vulnerable persons.

5.8 Health, Safety & Security

- Follow risk assessments, safety briefings, and incident procedures; report accidents/near misses.
- **No alcohol/drugs** while on duty or when responsible for beneficiaries/events.

5.9 Political Activity & Public Statements

- Personal political views must not be represented as those of the Organization.
- Media statements require authorization from the Executive Director or designated spokesperson.

5.10 Use of Position & Resources

- Do not use your role to obtain personal benefits or to disadvantage others.
 - **No retaliation** against complainants, witnesses, or investigators.
-

6) Reporting & Whistleblowing (Confidential; Good-Faith)

6.1 Duty to Report

All personnel and partners must report suspected or actual breaches of this Code, safeguarding, PSEA, fraud/corruption, or data protection incidents. Good-faith reporters are protected.

6.2 Handling of Reports

- Acknowledge receipt (if reporter known) within 2 working days.
 - Triage and protection measures within 5 working days; refer to appropriate policy (safeguarding/SEA) as needed.
 - Maintain confidentiality and records in the Ethics Register; share on a need-to-know basis only.
-

7) Investigations & Consequences

- Investigations are conducted by trained, conflict-free personnel (internal or external) under ToR; fair process for all parties.
 - **Sanctions** (depending on severity): coaching/warning; training; restitution; suspension; reassignment; **termination**; contract remedies for partners/vendors; **referral to authorities** for criminal conduct.
 - **Knowingly false, malicious allegations** may lead to disciplinary action; **good-faith** reporters remain protected even if concerns are not substantiated.
-

8) Training, Acknowledgement & Records

- Mandatory induction and **refresher training** at least every **24 months**.
 - All personnel/significant partners sign **Annex A - Acknowledgement & Annual Declaration**.
 - ECO maintains training and declaration records.
-

9) Monitoring, Learning & Review

- Quarterly management review of incidents and trends (anonymised); report to National Board annually.
 - Lessons learned feed updates to procedures and training.
 - **Annual review** of this Code or earlier after legal/operational changes.
-

10) Policy Communication & Accessibility

- Publish internally (and externally where appropriate); provide translations (LT/RU/EN).
 - Display **poster text** for reporting channels at offices/venues and on the website.
-

Annexes (Templates)

Annex A — Acknowledgement & Annual Declaration

I confirm that I have received, read, and understood the **Code of Conduct** and agree to comply. I declare below any actual/potential **conflicts of interest** or safeguarding concerns (or write “none”) and will promptly report any changes.

Signature: _____ Name: _____ Role: _____ Date: _____

Annex B — Conflict of Interest (COI) Disclosure Form

- Nature of interest/relationship:

- Parties involved:

- Role in any related decision/procurement:

- Proposed mitigation (recusal, reassignment, firewall):

- ECO decision/notes:

Signature: _____ Date: _____

Annex C — Gifts & Hospitality Register

Date	Offered by	Description	Approx. value (€)	Accepted/ Declined	Pre-approval (Y/N)	ECO notes

Chapter 2. Complaints & Whistleblowing Policy

Related policies: Incident Reporting & Case Management SOP; Code of Conduct; Non-Discrimination & DEI Policy; Child Protection & Safeguarding

Policy; SEA Prevention & Response Policy; Duty of Care Policy; Travel & Field Safety Policy; GDPR & Data Protection Policy; Privacy Policy; Data Breach Response Plan; IT & Cybersecurity Policy; Records Retention & Destruction Schedule; Fraud Response Plan; Conflict of Interest (COI) Policy; Procurement & Ethical Purchasing Policy; Media, Storytelling & Image Consent Policy; Infiltration & Internal Surveillance Policy; Partner Due Diligence & Vetting SOP; Partner Disclosure Policy; Sustainability Guidelines.

1) Purpose & Scope

This Policy provides a clear, safe, and accessible framework for raising and resolving complaints and whistleblowing disclosures. It ensures that concerns are handled fairly, confidentially, without retaliation, and in compliance with law (including the EU Whistleblowing Directive (EU) 2019/1937 and Lithuanian law), safeguarding duties, and GDPR.

Who can use it: staff, volunteers, interns, Board members, contractors/consultants, suppliers, implementing partners, beneficiaries/service users, and visitors.

What it covers:

- **Complaints:** dissatisfaction about our services, staff conduct, decisions, or how we applied policy.
 - **Whistleblowing (Protected Disclosures):** good-faith reporting of suspected wrongdoing in the **public interest** (e.g., fraud/corruption, criminal conduct, serious breach of law/policy, SEA/safeguarding abuse, health & safety risks, environmental damage, data protection breaches, conflict of interest/infiltration, cover-ups).
 - Not for: routine employment grievances (handled via HR procedures), except where they involve public-interest wrongdoing.
-

2) Principles

1. **Do No Harm & safety first**—especially for survivors, children, and at-risk persons.
2. **Non-retaliation**—strictly prohibited; we protect good-faith reporters and witnesses.

3. **Confidentiality & GDPR**—identity protected on a **need-to-know** basis; minimal data processing.
 4. **Fairness & due process**—impartial handling; right to be heard; proportionate actions.
 5. **Accessibility & inclusion**—multiple languages, formats, and reasonable accommodations.
 6. **Timeliness & transparency**—acknowledge, update, and close within defined timeframes.
 7. **Learning & accountability**—track trends, correct issues, and improve systems.
-

3) Definitions (Plain Language)

- **Complaint:** an expression of dissatisfaction (service, decision, behaviour) seeking a response or remedy.
 - **Whistleblowing / Protected Disclosure:** disclosure of information about suspected wrongdoing in the public interest by someone with a work-related connection.
 - **Reporter/Complainant/Whistleblower:** the person raising the concern.
 - **Respondent:** person or unit whose conduct/decision is complained about.
 - **Retaliation:** any adverse action or threat because a person made or assisted a report in good faith.
 - **Good faith:** honest belief that the information is true at the time, whether or not later substantiated.
-

4) Roles & Responsibilities

- **National Board:** oversight of Policy; receives anonymised trend reports; acts as escalation point where ED is implicated.
- **Executive Director (ED):** accountable for implementation/resources; approves sanctions and high-risk decisions.

- **Ethics & Compliance Officer (ECO): Policy owner;** manages **Complaints & Whistleblowing Register;** triages cases; assigns Case Lead; ensures non-retaliation.
- **HR & People and Culture Lead:** manages workplace conduct complaints and employment-grievance interface.
- **DSL/CPO & PSEA Focal Point:** lead on safeguarding/SEA; survivor-centred approach; legal referrals.
- **DPO:** ensures privacy/GDPR compliance; handles data-protection complaints and breach notifications.
- **IT & Security Lead:** handles cyber/IT issues and evidence handling.
- **Managers/Programme Leads:** cooperate with inquiries; implement corrective actions.
- **All personnel & partners:** report concerns promptly; preserve evidence; cooperate with investigations.

Designated contacts (to fill): ECO; HR Lead; DSL/CPO; PSEA FP; DPO; IT Lead; **complaints inbox:** *complaints@adliga.fund*; **whistleblowing inbox:** *whistleblow@adliga.fund*; **Board Chair contact** for escalation.

5) Reporting Channels

- **Email/webform inboxes** (complaints & whistleblowing) and **anonymous box/hotline.**
- Direct to **ECO, HR, DSL/PSEA, DPO, any manager,** or **Board Chair** if ED implicated.
- Multiple languages and accessible formats; interpreters where feasible.

External options (when applicable): competent authorities/regulators, law enforcement, donors. Complainants can seek external advice at any time.

6) Process Overview & Timeframes

6.1 Intake & Registration

- Log in **Register** (minimal personal data). Assign **Case ID.**

6.2 Acknowledgement

- **Within 7 days** for whistleblowing (EU standard).
- **Within 2 working days** for complaints; **same day** for **safeguarding/SEA/child protection** or immediate safety risk.

6.3 Triage & Risk Assessment

- Classify (complaint vs. protected disclosure). Rate severity (Low/Medium/High/Critical). Identify conflicts of interest. Implement immediate safety measures if needed.

6.4 Resolution Path

- **Early resolution** (minor service issues) within **10 working days** where appropriate.
- **Formal investigation** for serious/complex matters per **Incident Reporting & Case Management SOP**.

6.5 Updates & Feedback

- Provide **reasonable updates** at key stages. For whistleblowing, give **feedback within 3 months** (status/outcome, respecting privacy/law).

6.6 Closure & Learning

- Written outcome with reasons and any **Corrective Action Plan (CAP)**. Capture lessons learned.
-

7) Confidentiality, Data Protection & Anonymity

- We accept **anonymous reports**; limitations will be explained.
- Reporter identity kept confidential except where law requires disclosure or necessary to ensure a fair process—decided case-by-case with **ECO/DPO**.
- Process only **minimum necessary** data; store Case Files in restricted DMS; encrypt sensitive files; maintain access logs.
- Respect data-subject rights with necessary restrictions to protect investigations/third-party rights.

Retention: complaints **5 years after closure**; whistleblowing/serious misconduct **10 years**; safeguarding/SEA & child cases per Safeguarding Policy (longer where specified). Cross-reference **Records Schedule**.

8) Non-Retaliation & Support

- Any retaliation (threats, harassment, demotion, dismissal, blacklisting) against good-faith reporters/witnesses is a breach of this Policy and may result in disciplinary measures up to termination and referral to authorities.
 - Offer appropriate support and accommodations (e.g., schedule changes, supervision changes, counselling referrals).
 - Maintain a Retaliation Watch and follow-up at 30/60/90 days (Annex H).
-

9) Investigation Standards

- Impartial investigators; declare conflicts; trauma-informed interviews; secure evidence and chain of custody; follow Incident SOP timelines and documentation standards.
 - Right to be heard for respondents; confidentiality and data protection maintained for all parties.
-

10) Decisions, Remedies & Appeals

- Outcomes may include: apology; service change; training; CAP; supervision changes; sanctions (warning, suspension, termination); contract remedies; referral to authorities/regulators; donor notifications.
 - **Appeals:** Complainant/whistleblower may appeal within **10 working days** of outcome; reviewed by an independent senior manager/Board delegate (Annex G). Decision communicated in writing.
-

11) Communications & Transparency

- External communications require ED/Comms approval and must protect privacy.

- Publish aggregated, anonymised annual statistics (e.g., number of cases, types, time to close, corrective actions) to promote transparency and learning.
-

12) Training, Awareness & Accessibility

- Induction for all staff/volunteers; annual refreshers for managers and focal points.
 - Promote channels (posters/QR codes, intranet, partner packs); provide plain-language guides in LT/RU/EN where possible; ensure accessible formats.
-

13) Monitoring, KPIs & Audit

- KPIs (quarterly): acknowledgment within SLA; feedback $\leq$ 3 months; case closure time by severity; CAP completion; retaliation incidents; training completion.
 - Spot audits of Case Files and Register; annual report to the National Board.
-

14) Review & Continuous Improvement

- ECO reviews this Policy annually or after significant legal/practice changes; updates are communicated to all personnel and partners.
-

Annexes (Templates & Tools)

Annex A — Complaint Form (Service/Conduct/Decision)

- Reporter; contact; language/access needs; description; desired outcome; supporting evidence; consent preferences.

Annex B — Whistleblowing Report (Protected Disclosure)

- Reporter (or anonymous); role; facts; when/where; persons involved; evidence; public-interest nature; prior steps taken; retaliation risk.

Annex C — Acknowledgement Templates

- Complaint (≤ 2 working days); Whistleblowing (≤ 7 days); safeguarding/SEA (same day).

Annex D — Triage & Risk Assessment Sheet

- Type; severity; safety measures; conflicts; assigned Case Lead; next steps.

Annex E — Investigation Plan & Interview Notes

- Scope; witness list; evidence; timelines; interview guide; chain-of-custody link.

Annex F — Outcome Letter Template

- Findings; decisions; remedies; CAP; appeal instructions; privacy note.

Annex G — Appeal Form & Procedure

- Grounds; requested remedy; panel; timeline; decision record.

Annex H — Retaliation Watch & Support Log

- Follow-ups at 30/60/90 days; support offered; status; escalation if issues arise.

Annex I — Register Fields (Complaints & Whistleblowing)

- Case ID; date; type; severity; SLA flags; actions; CAP; outcome; appeal; retention timer.

Annex J — Privacy Notice for Complaints & Whistleblowing (GDPR Art. 13/14)

- Controller; purposes; lawful bases; recipients; transfers; retention; rights; contact; complaints to supervisory authority.

Chapter 3. Conflict of Interest (COI) Policy

Related policies: Code of Conduct; Anti-Fraud & Corruption; Procurement Policy; Child Protection & Safeguarding; Sexual Exploitation & Abuse (SEA) Prevention & Response; Data Protection/Privacy; Whistleblowing & Complaints Procedure; Partner & Vendor Due Diligence Standards.

1) Policy Statement & Purpose

The Organization is committed to objective, fair, and accountable decision-making free from undue influence. Conflicts of interest (COI)—actual, potential, or perceived—must be disclosed, assessed, and managed to protect integrity, donor confidence, public trust, and program quality.

Objectives:

- prevent improper advantage and unethical behaviour;
 - ensure decisions serve the best interests of the Organization;
 - provide clear disclosure, review, mitigation, and documentation processes;
 - align with law, donor rules, and good governance standards.
-

2) Scope & Applicability

Applies to all associated with the Organization: employees (permanent/temporary), volunteers, interns, National Board members, consultants, contractors, suppliers, implementing partners, and—where relevant—donors/beneficiaries interacting with our governance and procurement processes. Compliance is a condition of engagement.

3) Definitions (Plain Language)

- **Conflict of interest (COI):** a situation in which personal interests (financial, familial, professional, political or other) could **improperly influence—or appear to influence—** the person's duties or decisions.
- **Actual COI:** the conflict exists now.
- **Potential COI:** the conflict may arise in the future.
- **Perceived (apparent) COI:** a reasonable observer could believe that interests may improperly influence decisions.
- **Related party / close associate:** spouse/partner, child, parent, sibling, in-law, household member, or any person with whom there is a close personal, fiduciary, or business relationship.

- **Self-dealing:** using one's role to benefit oneself or a related party.
- **Recusal:** withdrawing from access, discussion, decision, and vote on a matter due to COI.

Examples (non-exhaustive):

- **Financial:** ownership/interest in a vendor; fees/commissions; using Organization assets for personal gain.
 - **Relationships:** supervising a relative; awarding contracts to friends/family; nepotism/favouritism.
 - **Gifts & hospitality:** expensive gifts, trips, or entertainment from suppliers/partners/donors.
 - **External roles:** board/employment with entities that contract with or compete with the Organization; diversion of opportunities, funds, or IP for external gain.
 - **Confidential information:** use or disclosure for personal/third-party benefit.
-

4) Roles & Responsibilities

- **National Board:** approves this Policy; oversees COI management; reviews high-risk/Board-level cases; ensures annual declarations; receives an annual COI report.
- **Executive Director (ED):** implements Policy; ensures training; appoints an **Ethics & Compliance Officer (ECO)**; escalates serious cases to the Board.
- **Ethics & Compliance Officer (ECO):** primary intake and advice; maintains the **COI Register** and **Gifts & Hospitality Register**; coordinates assessments/mitigations; records recusals and decisions; safeguards non-retaliation.
- **Managers & Project Leads:** ensure disclosures in teams; prevent conflicted assignments; embed COI checks in procurement/hiring.
- **Procurement & Finance Leads:** enforce competition rules, vendor due diligence, and related-party checks.

- **All personnel, partners, and Board members:** disclose COIs **promptly**; avoid conflicted decision-making; comply with mitigations and recusals.
-

5) Standards & Prohibitions

- **No self-dealing:** do not use your role to benefit yourself/related parties.
 - **No nepotism/favouritism:** hiring, promotions, appraisals, and procurement must be merit-based and competitive.
 - **Gifts & hospitality (aligns with Code of Conduct):**
 - Accepting gifts/hospitality **over €50 per item or €100 total per year per source** requires prior **written approval** and entry in the Register.
 - **Prohibited:** cash/cash equivalents; gifts during active tenders; anything that could influence—or appear to influence—decisions.
 - **Outside employment/board roles:** disclose in advance; obtain written approval if role interfaces with the Organization; implement mitigations (recusal/firewalls).
 - **Confidential information & opportunities:** never use for personal or third-party gain; no unauthorised disclosure.
 - **Political/advocacy activities:** personal views are personal; do not use Organization resources or name to support parties/candidates.
-

6) Disclosure Requirements

6.1 Annual Declarations

- All Board members, senior staff, project leads, procurement/finance roles, and staff with spending authority complete **Annex A - Annual COI Declaration** by **31 January** each year (or on onboarding) and update within **10 business days** of any change.

6.2 Ad Hoc Disclosures

- Any person who identifies an actual/potential/perceived COI must **immediately (within 5 business days)** submit **Annex B - Ad Hoc Disclosure** to the ECO and **verbally declare** the COI at the start of the relevant meeting.

6.3 Meeting Protocol

- The chair ensures disclosures are minuted using **Annex C - Recusal Statement**. The conflicted individual **leaves the room** (physical/virtual) for the item and **does not receive papers** for that item.

6.4 Procurement & Hiring

- Disclose any relationships to vendors/candidates **before** shortlisting; conflicted individuals must not participate in scoring, negotiation, or award decisions.

6.5 Confidentiality & Non-Retaliation

- Disclosures are handled confidentially and logged in the COI Register. Good-faith disclosures are protected from retaliation.

7) Assessment, Mitigation & Decisions

Process:

1. **Intake & triage (ECO):** confirm facts; classify risk (low/med/high).
2. **Mitigation proposal:** recusal, reassignment, “Chinese wall” (information barrier), independent review, divestment, contract safeguards, or termination of conflicted arrangement.
3. **Decision:** ED for staff/operational cases; **National Board** (or its Audit/Ethics Committee) for Board-level/material cases.
4. **Documentation:** record in COI Register; minute recusal/decision; notify parties; monitor compliance.

Appeal on process grounds may be lodged to the Board Chair within **10 business days**.

8) Procurement & Hiring Controls (Consistency with Policies)

- **Competition:** at least **3 quotes** (where feasible) for purchases above internal thresholds; technical and financial criteria defined in advance; records retained.
 - **Related-party transactions:** permitted only with **full disclosure, documented best-value assessment**, and prior written approval by ED/Board.
 - **Panels:** diverse, conflict-free selection panels; members sign COI statements prior to evaluation.
 - **No supervision of close relatives** (direct line management prohibited); alternative line management must be arranged if employment is justified.
 - **Debarment:** vendors or individuals breaching COI rules may be excluded from future opportunities.
-

9) Records, Registers & Data Protection

- **COI Register** (owned by ECO): annual and ad hoc disclosures, decisions, and mitigations; access on a **need-to-know** basis.
 - **Gifts & Hospitality Register:** maintain per Code of Conduct.
 - **Minutes:** Board Secretary records disclosures/recusals for agenda items.
 - **Retention:** keep COI and Gifts records **5 years** (or longer if legally required); process personal data per Privacy Policy/GDPR.
-

10) Enforcement & Sanctions

- Failure to disclose/manage a COI, interference with the process, or retaliation may result in disciplinary action (warning, training, removal from role, termination), contract remedies for partners/vendors, and/or referral to authorities if criminal/fraud concerns arise.
 - Good-faith reporters are protected; malicious or knowingly false allegations may themselves be subject to discipline.
-

11) Training, Acknowledgement & Review

- Induction and refresher training (at least every 24 months) for all personnel; annual briefings for Board.
 - Annual Acknowledgement & Declaration signatures collected and archived by ECO.
 - Annual management summary to the National Board; Policy review at least annually or after incidents/changes.
-

12) Policy Communication & Accessibility

- Publish internally; provide translations (LT/RU/EN); post **how to disclose** instructions and contacts in offices and staff handbook.
 - Ensure easy access to forms and registers for authorised users.
-

Annexes (Templates)

Annex A — Annual COI Declaration (Board/Staff)

- Name/Role/Department:

 - List any external positions (paid/unpaid):

 - Financial interests (companies/securities/assets relevant to our work):

 - Related parties (close associates) with links to our vendors/partners/donors: _____
 - Gifts & hospitality over thresholds received in past 12 months:

 - Other relationships or interests that could appear to influence decisions: _____
- I declare that the above is complete and I will update ECO within 10 business days of any change.
- Signature: _____ Date: _____
-

Annex B — Ad Hoc COI Disclosure (Event/Decision-Specific)

- Person disclosing / role: _____
 - Agenda/item / procurement or hiring reference:

 - Nature of conflict (financial/relationship/gift/external role/other):

 - Proposed mitigation (recusal, reassignment, firewall, independent review): _____
 - ECO initial assessment (risk level; next steps):

Signature (person): _____ Date: _____ ECO: _____ Date: _____
-

Annex C — Recusal Statement & Minutes Note (for Chair/Secretary)

- Meeting/body: _____ Date: _____ Item: _____
 - Person recused: _____ Nature of COI:

 - Recusal scope: ☐ no papers received ☐ absent for discussion ☐ absent for decision/vote
 - Decision authority & outcome:

 - Follow-up/mitigations to monitor:

Secretary signature: _____ Date: _____
-

Annex D — Gifts & Hospitality Register (Cross-ref: Code of Conduct Annex C)

Date	Offered by	Description	Approx. value (€)	Accepted/ Declined	Pre-approval (Y/N)	ECO notes

Annex E — Mitigation Plan Template (for Medium/High-Risk COI)

- Risk summary & context:

- Controls: recusal scope; information barriers; independent oversight; rotation; reporting cadence.
- Owner(s) & timeline:

- Review checkpoints & success criteria:

- Closure decision (ED/Board):

Chapter 4. Policy on Preventing Infiltration by State Security Agents and Internal Surveillance of Activists

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

1) Policy Statement & Purpose

The Organization is committed to protecting activists, beneficiaries, staff, volunteers, and partners from risks arising from infiltration by hostile state security services or their proxies, and from unauthorised internal surveillance (covert recording/monitoring) that could endanger people or undermine our mission. This Policy defines lawful, rights-respecting,

risk-based controls to prevent, detect, and respond to such threats while upholding human rights, GDPR, and Lithuanian law.

Objectives: (a) reduce exposure of sensitive information and people; (b) deter and detect infiltration and covert monitoring; (c) respond safely and proportionately; (d) ensure accountability, non-retaliation, and due process.

2) Scope & Applicability

Applies to all personnel and associated parties: employees, volunteers, interns, National Board members, consultants, contractors, suppliers, implementing partners, visitors, and any third parties engaged in our activities or accessing our information or premises.

3) Definitions (Plain Language)

- **Infiltration:** intentional attempt by a hostile actor to gain access (employment, volunteering, partnership, events, online spaces) to collect information, influence decisions, disrupt programmes, or target individuals.
 - **Internal surveillance:** unauthorised monitoring, recording, photographing, or data collection inside our activities/spaces without proper notice, consent, or legal basis.
 - **Hostile actor:** state security service, affiliated organisation, or proxy acting on their behalf; or any party acting to harm people, programmes, or data.
 - **Insider threat:** a person with legitimate access who intentionally or negligently causes harm (e.g., data exfiltration, covert recording, social engineering).
 - **Social engineering:** deception to obtain information, access, or influence decisions (phishing, pretexting, tailgating).
 - **Need-to-know:** access only to the minimum information required to perform one's role.
-

4) Principles

1. **Legality & human rights:** actions must be lawful, necessary, and proportionate; no vigilantism or discrimination.
 2. **Do No Harm & safeguarding:** prioritise safety of activists and beneficiaries; consult Safeguarding leads where risks to vulnerable persons exist.
 3. **Privacy by design (GDPR):** minimise data; transparent, documented monitoring only where lawful and announced.
 4. **Non-discrimination:** risk controls are behaviour- and risk-based, **never** based on nationality, ethnicity, religion, or protected characteristics.
 5. **Accountability & due process:** fair investigations, documented decisions, and right to be heard where appropriate.
 6. **Least privilege & need-to-know:** restrict access to reduce impact of compromise.
 7. **Non-retaliation:** protect good-faith reporters and witnesses.
-

5) Roles & Responsibilities

- **National Board:** approves this Policy; receives incident summaries and risk reports; oversees corrective actions.
- **Executive Director (ED):** accountable for implementation; appoints **Insider Threat/Integrity Program Lead** (the **Ethics & Compliance Officer, ECO**); authorises emergency restrictions and law-enforcement liaison.
- **Ethics & Compliance Officer (ECO):** primary intake for concerns; maintains **Integrity Incident Register**; coordinates investigations with HR/DPO/IT; enforces non-retaliation.
- **IT & Security Lead:** manages digital/physical security, monitoring per law, access reviews, incident response, and forensics; maintains **Access & System Registers**.
- **Data Protection Officer (DPO):** ensures GDPR compliance; maintains ROPA; advises on DPIAs/TIAs; co-leads breach assessment and notifications.

- **HR/People & Culture:** conducts lawful, non-discriminatory vetting; manages joiner-mover-leaver (JML); ensures training.
- **Programme Leads/Managers:** apply need-to-know access; validate guest lists; ensure safe meetings and events.
- **Safeguarding Leads (DSL/CPO & PSEA Focal Point):** advise where content involves children/SEA or vulnerable persons.
- **Comms Lead:** manages media access, event signage, and takedowns; handles sensitive inquiries.
- **All personnel & partners:** follow this Policy; report concerns immediately; protect information; avoid unauthorised recording.

Designated Contacts (to fill): ECO; IT & Security Lead; DPO; HR Lead; DSL/CPO; Comms Lead; **incident inbox:** *integrity@adliga.fund*.

6) Risk Assessment & Planning

- Maintain an annual Threat & Risk Assessment identifying programmes/roles at higher risk (e.g., activism, legal support, survivors).
 - Maintain a Risk Register with owners, mitigations, and review dates.
 - For new projects/events/tools, perform DPIA and (if needed) Security Risk Assessment before launch.
 - Classify information and label sensitive materials; avoid unnecessary personal identifiers.
-

7) Vetting, Onboarding & Partnerships (Lawful; Non-Discriminatory)

- Pre-engagement checks proportionate to role risk: identity verification; right-to-work; gaps in CV; two references; COI declarations; public-domain red flags (no intrusive OSINT beyond legitimate interest).
- For high-risk roles: additional verification (e.g., credential checks) with DPO/ECO approval.

- Partner due diligence: legal status, leadership, sanctions/PEP screening (where relevant), safeguarding/privacy standards, and past conduct.
 - All personnel sign Confidentiality/AUP; complete security & privacy induction.
-

8) Access Control & Sensitive Meetings

- Least privilege: RBAC enforced; quarterly access reviews; two-person integrity for critical actions.
 - Visitor management: pre-registration, ID check where appropriate, visitor badges, escorted access; visitor NDA/Notice for sensitive areas.
 - Sensitive meeting protocol: invite-only; verify attendees; disable unauthorised recording; store minutes securely; use Chatham House Rule where appropriate; phones on silent or placed away if agreed.
 - No covert recording: any recording must be announced and consented to; hidden devices prohibited.
-

9) Communications & Information Handling

- Use approved, encrypted communication tools with MFA; verify identities out-of-band for unusual requests.
 - Mark and share information per classification; avoid sharing personal data via unmanaged channels; use secure links not attachments.
 - Remove geotags/EXIF from sensitive photos; avoid precise locations for at-risk persons; follow the Media Policy.
 - Prohibit forwarding of internal emails/chats outside authorised channels; restrict mass exports and downloads.
-

10) Events, Outreach & Field Work

- Conduct pre-event risk checks; confirm media policy/signage; provide opt-out mechanisms.

- Limit publishing of attendee lists; anonymise participant identifiers where possible.
 - Assign a Duty Officer for security escalation; maintain incident and first-aid contacts.
-

11) Red Flags (Non-exhaustive)

- Persistent requests for privileged/access-only information without need-to-know.
- Attempts to bypass procedures (tailgating, pressuring staff for shortcuts).
- Unauthorised recording/photography in sensitive areas or meetings.
- Creation of parallel/“shadow” communication groups or document stores.
- Anomalous data activity (mass exports, unusual logins) or refusal to use approved tools.
- Undisclosed outside affiliations relevant to our work; unexplained funding offers or gifts.
- Contact patterns consistent with social engineering or grooming.

Report red flags immediately to ECO/IT/DPO. Do not confront suspected individuals directly if it risks safety; prioritise containment and documentation.

12) Reporting, Non-Retaliation & Support

- Use confidential channels: ECO (primary), integrity@ inbox, anonymous webform/box/hotline, or Board Chair if ED is implicated.
 - Good-faith reporters and witnesses are protected; retaliation is prohibited and sanctioned.
 - Provide support to affected activists (safety planning, referrals to counselling/legal aid where available).
-

13) Response & Investigations (Due Process)

- Triage within 24 hours; secure evidence (logs, CCTV where lawful); restrict access as necessary.
- Investigations are fair, confidential, and proportionate; led by ECO with DPO/IT/HR; external counsel/authorities engaged where appropriate.
- Where criminal conduct is suspected, liaise with law enforcement; preserve chain of custody.
- Outcomes may include coaching, access changes, reassignment, disciplinary measures, vendor/partner remedies, or termination—consistent with law and contracts.

Linkages: data exposure handled per **Data Breach Response Plan**; financial irregularities per **Fraud Response Plan**; safeguarding matters via **Child Protection/SEA** procedures.

14) Monitoring & Privacy (Transparency)

- Any technical monitoring of systems (e.g., security logs, DLP alerts) is announced, proportionate, and for security purposes only, with DPO oversight and documented legal basis.
 - No covert employee surveillance; secret monitoring is prohibited except where strictly required by law with appropriate authorisation.
-

15) Training & Awareness

- Mandatory induction and 24-month refreshers on insider threat awareness, social engineering, secure meetings, and privacy.
 - Targeted exercises for high-risk teams (Comms, Programmes, IT, HR) and table-top simulations at least annually.
-

16) Sanctions & Remedies

- Violations may result in warnings, removal of access, suspension, termination, reporting to authorities, partner/vendor debarment, and contractual remedies.
- False or malicious allegations may themselves lead to disciplinary action.

17) Review & Continuous Improvement

- Post-incident lessons learned feed into updated controls; Policy reviewed annually or after major incidents or legal changes; summary shared with the National Board.
-

Annexes (Templates & Checklists)

Annex A — Integrity/Insider Threat Intake Form

- Reporter (name/anonymous); date/time; description; persons involved; location; evidence; immediate risks; actions taken; case ID.

Annex B — Sensitive Meeting Protocol & Checklist

- Invite control; identity verification; no-recording reminder; device management; seating/privacy; minutes circulation; storage path; approvals.

Annex C — Event Security & Media Signage Pack

- Photography/filming notice; opt-out badge/area; press check-in; emergency contacts; incident log template.

Annex D — Partner & Visitor NDA/Notice

- Confidentiality scope; permitted uses; retention; return/destruction; sanctions for breach.

Annex E — Access Review & JML Checklist

- Quarterly access attestations; privileged access review; leaver deprovisioning within 1 business day; shared mailbox audit.

Annex F — Social Engineering & COMSEC Quick Guide

- Verification steps; red flags; secure channel list; reporting steps; do's/don'ts.

Annex G — Incident Response Playbook (Integrity Cases)

- Triage; containment; evidence preservation; risk/effects; decision tree (notify DPO/Police/Donor); communications plan; closure.

Annex H — Do No Harm Assessment (At-Risk Activists)

- Threats, exposure points, travel/online risks; mitigation plan; contact protocol; consent considerations.