Data Protection & Privacy (GDPR)

1. **GDPR & Data Protection Policy**
2. **Privacy Policy**
3. **IT & Cybersecurity Policy**
4. **Data Breach Response Plan**
5. **Records Retention & Destruction Schedule**
6. **Media, Storytelling & Image Consent Policy**
7. **Cookie Policy**

Approved by: National Board

Updated: 2026-03-01

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

Chapter 1. GDPR & Data Protection Policy

Related policies: Privacy Policy; Information Security/IT Policy; Records Management & Data Retention; Whistleblowing & Complaints; Code of Conduct; Conflict of Interest (COI); Procurement & Ethical Purchasing; Financial Policy; Fraud Response Plan; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI.

---

1) Policy Statement & Purpose

This Policy sets out how the Organization complies with the EU General Data Protection Regulation (GDPR) and applicable laws of the Republic of Lithuania when collecting, using, sharing, securing, and retaining personal data. It establishes principles, roles, and procedures to protect individuals' rights and to ensure lawful, fair, and transparent processing.

Objectives: (a) embed data protection by design and by default; (b) manage risks via DPIAs, security controls, and retention; (c) honour data subject rights; (d) govern processors and international transfers; (e) respond effectively to incidents within legal timelines.

2) Scope & Applicability

This Policy applies to all processing of personal data conducted by or on behalf of the Organization, in any format (digital, paper) and location. It covers all associated persons: employees, volunteers, interns, National Board members, consultants, contractors, suppliers, implementing partners, and visitors interacting with our systems and programmes.

---

3) Legal Framework & Definitions

Framework: GDPR; Lithuanian data protection law and guidance from the **State Data Protection Inspectorate**; relevant EU guidance.

Definitions (plain language):

- **Personal data:** any information relating to an identified or identifiable person.
- **Processing:** any operation on personal data (collection, storage, use, sharing, erasure, etc.).
- **Controller:** the Organization that determines purposes and means of processing.
- **Processor:** a service provider processing data on our behalf under a contract.
- **Special category data:** sensitive data (e.g., health, biometric, racial/ethnic origin, political opinions, religion/belief, sexual life/orientation).
- **Pseudonymization / Anonymization:** techniques that reduce identifiability; anonymized data are no longer personal data.
- **Data subject:** the individual whose data are processed.
- **DPIA:** Data Protection Impact Assessment to assess high-risk processing.
- **ROPA:** Record of Processing Activities maintained under GDPR Art. 30.

- **Personal data breach:** security incident leading to accidental/unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

---

4) GDPR Principles (Art. 5)

We process personal data according to these principles:

1. **Lawfulness, fairness, transparency**
2. **Purpose limitation** (specific, explicit, legitimate purposes)
3. **Data minimisation** (adequate, relevant, limited)
4. **Accuracy** (kept up to date)
5. **Storage limitation** (kept no longer than necessary)
6. **Integrity & confidentiality** (security)
7. **Accountability** (we document and can demonstrate compliance)

---

5) Roles & Responsibilities

- **National Board:** approves this Policy; ensures resources; receives annual privacy/security reports and serious incident notifications.
- **Executive Director (ED):** overall accountability; ensures implementation and culture; escalates significant risks to Board.
- **Data Protection Officer (DPO):** independent advice and monitoring; point of contact for data subjects and the supervisory authority; oversees DPIAs, ROPAs, breach handling; no conflicts of interest.
- **Ethics & Compliance Officer (ECO):** manages complaints/whistleblowing and non-retaliation; coordinates with DPO for privacy-related matters.
- **IT & Security Lead:** implements technical and organisational security measures; access control; backups; logging; incident response.
- **Records Manager / FM/CA:** manages retention schedules and lawful bases tied to finance/records.

- **HR/People & Culture:** manages employee/volunteer data, recruitment transparency, and accommodation processes.
- **DSL/CPO & PSEA Focal Point:** handle safeguarding/SEA cases where special category data or children's data are involved.
- **Managers/Data Owners:** ensure lawful bases, notices, consent (where needed), and data quality in their areas.
- **All personnel & partners:** follow this Policy; complete training; protect data; report incidents promptly.
- **Processors:** operate under **Data Processing Agreements (DPAs)**; use sub-processors only with our written authorisation and equivalent safeguards.

Designated Contacts (to fill):

- **DPO:** *Name, phone, email*
- **IT & Security Lead:** *Name, phone, email*
- **ECO:** *Name, phone, email*
- **Privacy inbox:** *privacy@adliga.fund*

---

6) Lawful Bases & Transparency

We identify and document a lawful basis for each processing activity (contract, legal obligation, legitimate interests, consent, vital interests, public task where applicable).
We provide clear privacy notices (see Privacy Policy and Annex F templates) that explain purposes, legal bases, retention, sharing, and rights in plain language.

Consent: used where required; must be freely given, specific, informed, and unambiguous, evidenced by a record, and withdrawable at any time without detriment.

---

7) Records of Processing (ROPA)

The DPO maintains a central ROPA (Art. 30) covering all key processing contexts (supporters/donors, beneficiaries, employees/volunteers, vendors,

web/analytics, events). Data owners provide updates at least annually or upon changes. See Annex A (ROPA template).

---

8) Data Subject Rights & Requests (DSRs)

We enable rights of access, rectification, erasure, restriction, portability, objection, and consent withdrawal. Requests are logged and acknowledged within 7 days and fulfilled within one month (extendable by two months for complex requests with notice). Identity is verified where appropriate. Denials are documented with reasons and guidance on complaint routes.

See Annex I for the DSR workflow & log; Privacy Policy provides the public-facing process.

---

9) Privacy by Design & Default; DPIAs

Projects and systems must incorporate data protection from the outset. A DPIA is required where processing is likely high risk (e.g., special categories; vulnerable groups; systematic monitoring; large-scale processing; new technologies). DPIAs include consultation (where appropriate), risk analysis, mitigations, and DPO review. See Annex B (DPIA template) and Annex H (DPIA trigger questions).

Default settings should be privacy-protective (minimal data, least privilege access, opt-in tracking, limited retention).

---

10) Data Classification & Handling

We use four classes with handling rules (see **Annex C**):

- **Public** (shareable)
- **Internal** (Organization use only)
- **Confidential** (restricted access; encryption at rest/in transit)
- **Special Category/Highly Confidential** (strict access; encryption; additional approvals; no external sharing without DPO clearance)

Transmission & storage: encryption, secure file sharing, and approved platforms only; no personal accounts for Organization data.

Disposal: secure deletion/shredding; include backups per **Annex E** retention schedule.

---

11) Security Measures (TOMs)

- **Access control & RBAC** (role-based); **MFA** on critical systems; least privilege; periodic access reviews.
- **Encryption** in transit (TLS) and at rest (where supported).
- **Backups & continuity** with regular restore tests.
- **Secure configuration & patching**; malware protection; vulnerability management.
- **Logging & monitoring** of security events; incident response plan.
- **Physical security** (locked storage; visitor controls).
- **Portable media & remote work** controls; prohibition of unauthorised devices.
- **Supplier security** aligned with DPAs and due diligence.

---

12) Retention & Minimisation

We keep data no longer than necessary for stated purposes and legal requirements. Retention periods are defined in Annex E – Data Retention Schedule and aligned with Finance/HR policies. At end of retention, data are deleted or anonymised; deletion from backups is handled per backup lifecycle.

---

13) Processors, Vendors & International Transfers

We appoint processors only after due diligence (see Annex F). DPAs include subject matter, duration, type of data, categories of data subjects, security measures, sub-processor conditions, assistance with rights, return/deletion of data, audits, and breach notifications.

International transfers outside the EU/EEA use valid mechanisms (e.g., EU–US Data Privacy Framework, Standard Contractual Clauses with

supplementary measures). A Transfer Impact Assessment (TIA) is completed where required (see Annex G).

---

14) Data Sharing & Disclosure

Sharing is **limited and proportionate**:

- **Internal**: on a need-to-know basis.
- **External**: with processors (per DPA), joint controllers (per arrangement), partners for joint activities (with clear roles), or authorities where required by law.
- Use **pseudonymisation/aggregation** where feasible; avoid unnecessary identifiers.

---

15) Incident & Breach Response (72-Hour Plan)

All personnel must report suspected incidents immediately to the DPO/IT. The DPO leads assessment with IT, ECO, and relevant leads to determine risk to individuals.

Where required, the Organization will notify the supervisory authority within 72 hours and affected individuals without undue delay. All breaches are recorded in the Breach Register. See Annex H – Breach Response Plan & Register and the Privacy Policy’s Breach Checklist.

---

16) Children’s Data & Safeguarding

Where programmes involve children, processing follows this Policy and our Child Protection & Safeguarding and SEA Policies. Parental/guardian consent (and child assent where appropriate) is obtained using approved forms; only minimum necessary data are processed.

---

17) Training & Awareness

Mandatory induction and refresher every 24 months for all personnel; role-based training for managers, HR, IT, finance, and safeguarding roles. Quarterly awareness (e.g., phishing drills, privacy tips). Training completion is recorded.

---

18) Monitoring, Audit & Review

The DPO conducts periodic reviews of ROPA, DPIAs, DPAs, retention, and breach/DSR logs. Independent or internal audits may be performed. An annual privacy report is submitted to the National Board. This Policy is reviewed at least annually or after major changes/incidents.

---

19) Non-Compliance & Sanctions

Breaches of this Policy may result in corrective actions, access restrictions, disciplinary measures up to termination, partner/vendor remedies (suspension, termination), and reporting to authorities where required.

Annexes (Templates & Standards)

Annex A — Record of Processing Activities (ROPA) Template

- Purpose; lawful basis; categories of data/subjects; recipients; transfers; retention; security measures; joint controller/processor roles; DPIA flag; last review.

Annex B — DPIA Template

- Project description; stakeholders; lawful bases; necessity/proportionality; risks to rights/freedoms; mitigations; consultation; residual risk; DPO opinion; decision.

Annex C — Data Classification & Handling Standard

- Classes (Public/Internal/Confidential/Special); storage, transmission, sharing, printing, and disposal rules; encryption requirements; approval flow for Special Category.

Annex D — Access Control Standard (RBAC/MFA)

- Role mapping; joiner-mover-leaver process; authentication; MFA coverage; privileged access; access reviews; logging.

Annex E — Data Retention Schedule (Summary)

- Donations/finance **10 years**; newsletters until unsubscribe; enquiries **3 years**; programme/event **5 years**; website logs **12 months**;

HR/finance per relevant policies; safeguarding/SEA per safeguarding policies.

Annex F — Processor Due Diligence & DPA Checklist

- Capabilities; security; sub-processors; location/transfers; incident history; insurance; DPA clauses; audit/cooperation rights.

Annex G — International Transfer Assessment (TIA) Template

- Destination, law/regime, risks, SCCs/DPF status, supplementary measures, decision.

Annex H — Breach Response Plan & Register

- Triage; containment; forensics; risk assessment; notifications; remediation; lessons learned; log fields.

Annex I — Data Subject Request (DSR) Workflow & Log

- Intake channel; identity verification; clock start; tasks; deadline; decision; communication; archive.

Annex J — Consent Management & Withdrawal Log

- Consent context; data subject; notice text; timestamp; method; withdrawal date; system updates.

Annex K — Photography/Media Consent (Adults & Children)

- Purpose, scope, withdrawal, storage, and safeguarding alignment; link to safeguarding annexes.

Annex L — Staff Privacy Notice (Employment) Outline

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

Annex M — CCTV/Access Control Register (if applicable)

- Locations; purpose; signage; retention; access; disclosures; DPIA; maintenance logs.

Annex N — Acknowledgement & Annual Declaration

“I confirm I have read and understood the GDPR & Data Protection Policy, will comply with it, and will complete required training.”
Signature: _____ Name: _____ Role: _____ Date: _____

Chapter 2. Privacy Policy

Related policies: Code of Conduct; Whistleblowing & Complaints; Data Retention & Records Management; Information Security/IT; Procurement & Ethical Purchasing; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI; Financial Policy; Fraud Response Plan.

---

1) Introduction & Controller Information

This Privacy Policy explains how we collect, use, disclose, store, and protect personal data when you interact with us—e.g., donate, subscribe to our newsletters, participate in our programmes, contact us, or use our websites (including adliga.fund).

Contact for privacy matters: *privacy@adliga.fund* (or DPO below).

Registered address: *Vilnius, Lithuania*

DPO (to fill): *Name, phone, email*

We process personal data in line with the EU General Data Protection Regulation (GDPR) and applicable Lithuanian law.

---

2) What Data We Collect (Categories)

Depending on your interaction, we may process:

- **Identity & contact data:** name, surname, email, phone, postal/billing address.
- **Donation & payment metadata:** donation amount, currency, date/time, method, transaction status, donation intent (campaign). **We do not store full card or bank credentials.**
- **Communication preferences:** newsletter opt-ins/opt-outs, topics, language.
- **Technical data:** IP address, device/browser type, pages viewed, cookies/analytics events (see **§10 Cookies & Analytics**).
- **Programme participation data:** event registrations, accessibility/accommodation needs (where provided), feedback forms.

- **Children's data (limited):** only where necessary for safeguarding/programme delivery and in accordance with law and our Safeguarding Policies.
- **Special category data: not intentionally collected** unless strictly necessary (e.g., accessibility needs) and processed with an appropriate lawful basis and safeguards.

---

3) Purposes & Legal Bases

We process personal data for the following purposes and legal bases under **GDPR Art. 6** (and **Art. 9** where applicable):

- **Process donations and issue receipts**; manage recurring gifts; acknowledge support.
  Legal bases: **contract/performance**, **legal obligation** (accounting/tax), **legitimate interests** (supporter stewardship, fraud prevention).
- **Operate newsletters and updates** you choose to receive; manage preferences.
  Legal bases: **consent**; **legitimate interests** (where permitted) for essential service emails.
- **Programme/event administration**, including registrations and accessibility arrangements.
  Legal bases: **contract/performance**, **legitimate interests**, **consent** (for specific accommodations).
- **Respond to enquiries and complaints**; measure service quality.
  Legal bases: **legitimate interests**.
- **Compliance, audit, and fraud prevention** (e.g., unusual activity screening).
  Legal bases: **legal obligation**, **legitimate interests**.
- **Website operation, security, and analytics.**
  Legal bases: **legitimate interests** (security, essential analytics) and **consent** (for non-essential cookies/analytics/marketing).

We do **not** engage in automated decision-making producing legal or similarly significant effects.

---

4) Payment Processing (Processors)

We use trusted third-party payment processors for secure transactions, such as Stripe and PayPal, and a donation management plugin (e.g., GiveWP) integrated with those processors. These providers act as processors (or independent controllers for certain activities) and handle your payment credentials directly under their own privacy terms. We receive transaction metadata (amount, date, status) but no full card/bank details.

---

5) Data Sharing & Recipients

We do **not** sell or rent personal data. We may share data with:

- **Service providers/processors** acting on our instructions (e.g., payment, email/newsletter, IT hosting, analytics, event tools) under data-processing agreements.
- **Professional advisors/insurers** (legal, audit) under confidentiality.
- **Public authorities/regulators** where required by law or to protect rights/safety.
- **Partner organizations** strictly for joint activities you choose to join, with transparency and appropriate safeguards.

---

6) International Data Transfers

Some processors may process data outside the EU/EEA (e.g., the United States). Where such transfers occur, we rely on an applicable transfer mechanism (e.g., EU–US Data Privacy Framework participation, Standard Contractual Clauses, and supplementary measures as needed).

---

7) Data Retention

We keep personal data **only as long as necessary** for the purpose, legal requirements, and our legitimate interests:

- **Donations/transactions:** typically **10 years** (accounting/tax rules).
- **Newsletter records:** until you **unsubscribe** or your account becomes inactive for a defined period.

- **Supporter enquiries:** typically **3 years** after closure.
- **Website logs/security data:** up to **12 months** unless needed longer for security/legal purposes.
- **Programme/event files:** typically **5 years** (or as contractually required).
  See **Annex C – Retention Schedule** for details.

---

8) Your Rights (GDPR)

You may have the right to access, rectify, erase, restrict, object to processing, data portability, and to withdraw consent where processing is based on consent. You also have the right to lodge a complaint with the State Data Protection Inspectorate in Lithuania. We will respond to verified requests within one month (extendable where permitted).

How to exercise your rights: use Annex A – Data Subject Request (DSR) Form or email privacy@adliga.fund. We may need to verify your identity.

---

9) Security Measures

We employ appropriate technical and organizational measures: encrypted connections (TLS/SSL); strong access controls and role-based permissions; secure configuration and backups; staff training; data minimisation; retention controls; vendor due diligence; incident response and breach procedures.

In case of a personal data breach likely to result in a risk to individuals, we will notify the supervisory authority within 72 hours and affected individuals where required by law.

---

10) Cookies, Analytics & Similar Technologies

We use cookies and similar technologies to operate our sites, remember preferences, measure traffic, and improve content.

- **Essential cookies**: required for site functionality and security.
- **Analytics cookies**: help us understand site usage; set **only with your consent**.

- **Marketing/third-party cookies**: used only where applicable and **only with your consent**.

You can manage preferences via our **Cookie Banner/Manager** and your browser settings. See **Annex D – Cookie Notice** for details (categories, retention, providers).

---

11) Email, Newsletters & Communications

We send newsletters only if you opt-in (or as otherwise permitted by law). You can unsubscribe at any time via the link in each email or by contacting us. We may send service messages (e.g., donation receipts, policy updates) that are not marketing.

---

12) Children's Privacy

Our public websites and donation forms are not directed to children. We do not knowingly collect data from children without appropriate consent as required by law. Where our programmes involve children, we apply our Child Protection and SEA Policies and obtain the necessary consents from parents/guardians.

---

13) Links to Other Sites & Social Media

Our sites may contain links to third-party websites or social media platforms. We are not responsible for their privacy practices. Please review their privacy notices.

---

14) Changes to this Policy

We may update this Policy from time to time. The "Updated" date above indicates the latest version. Significant changes will be communicated via our website or email where appropriate.

---

15) Contact Us

Questions or requests regarding privacy:

- **Email:** privacy@adliga.fund (or the DPO contact once designated)
- **Website:** adliga.fund

Annexes (Templates)

Annex A — Data Subject Request (DSR) Form

- Requester name/contact; relationship to Organization; request type (access/rectify/erase/restrict/object/portability/withdraw consent); details; ID verification check; response channel; deadline (1 month); handler and decision notes.

Annex B — Processor & Recipient Register

- Service; provider; country; role (processor/controller); data categories; legal basis; transfer mechanism; DPA/SCCs; retention; security summary; last review.

Annex C — Data Retention Schedule (summary)

- Donations/transactions – **10 years**;
- Newsletters – until unsubscribe/inactive;
- Enquiries/support – **3 years**;
- Programme files – **5 years**;
- Website logs – **12 months**;
- HR/finance records – per Finance/HR policies;
- Case files (safeguarding/SEA) – per Safeguarding Policies.

Annex D — Cookie Notice

- Categories (essential/analytics/marketing); examples; default durations; how to manage consent; link to Cookie Manager; third-party providers (analytics/email/embedded media) with purposes.

Annex E — Breach Response Checklist (72-Hour Plan)

- Detect & assess; contain; preserve evidence; notify DPO; risk evaluation; authority notification decision; data subject notification decision; remedial actions; lessons learned; update registers.

Annex F — Privacy Notice for Donors & Supporters (short form)

- Who we are; what we collect; purposes/legal bases; sharing; transfers; retention; rights; contact/unsubscribe; link to full Policy.

Annex G — Record of Processing Activities (ROPA) Outline

- Purpose; data categories; subjects; recipients; transfers; retention; security; lawful bases; DPIA flag; controller/processor roles.

Annex H — DPIA Trigger Questions

- Large-scale processing? Special category data? Vulnerable groups? Innovative tech? Cross-border transfers? Systematic monitoring? If “yes”, conduct DPIA.

Chapter 3. IT & Cybersecurity Policy

Policy owner: Executive Director / IT & Security Lead (with Data Protection Officer, DPO)
Related policies: GDPR & Data Protection Policy; Privacy Policy; Data Breach Response Plan; Records Retention & Destruction Schedule; Financial Policy; Procurement & Ethical Purchasing; Fraud Response Plan; Whistleblowing & Complaints; Code of Conduct; Conflict of Interest (COI); Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI; Business Continuity & Disaster Recovery (BCDR) Standard.

---

1) Policy Statement & Purpose

This Policy defines how we **protect information and systems** against loss, unauthorised access, misuse, or disruption. It sets **minimum security controls** for people, processes, and technology to ensure confidentiality, integrity, and availability of the Organization’s data, in line with **GDPR**, Lithuanian law, and donor/partner requirements.

Objectives: (a) reduce cyber risk; (b) safeguard beneficiaries, staff, and donors; (c) ensure resilient operations; (d) meet legal/contractual obligations; (e) promote a culture of security.

---

2) Scope & Applicability

Applies to **all information assets and systems** (on-prem, cloud/SaaS, mobile), and to all personnel and associated parties: employees, volunteers, interns, National Board members, consultants, contractors, suppliers, and implementing partners who access Organization information.

---

3) Roles & Responsibilities

- **National Board:** approves the Policy; receives annual security/privacy reports; oversees major risks and incidents.
- **Executive Director (ED):** accountable for implementation and resourcing; approves exceptions and major changes.
- **IT & Security Lead (CISO-equivalent):** defines controls/standards; manages risk register; leads vulnerability management, monitoring, and incident handling; maintains asset inventory.
- **Data Protection Officer (DPO):** ensures GDPR alignment; co-leads breach assessments; maintains Breach Register; advises on DPIAs/TIAs.
- **System/Data Owners:** ensure security of their applications and data; review access; maintain documentation.
- **Records Manager:** aligns retention and destruction with security controls.
- **Managers:** ensure team compliance, training completion, and joiner-mover-leaver actions.
- **All personnel & partners:** follow this Policy/AUP; protect credentials; report incidents immediately.
- **Vendors/Processors:** meet contractual security and privacy requirements; notify of incidents without delay.

Designated Contacts (to fill):

- **IT & Security Lead:** *Name, phone, email*
- **DPO:** *Name, phone, email*
- **Service Desk / Incident inbox:** *security@ / it@*

- **After-hours escalation:** *insert*

---

4) Information Classification & Handling

We classify information into **Public, Internal, Confidential, and Special Category/Highly Confidential** (see GDPR Policy Annex C). Handling rules:

- Store **Confidential** and **Special** data only in approved systems; encrypt **at rest and in transit**.
- Share on a **need-to-know** basis; use secure links instead of attachments where possible.
- Apply **clean desk** and **screen lock** practices; avoid printing unless necessary; secure shredding for disposal.

---

5) Acceptable Use of IT Resources (AUP)

- Organizational IT resources are for legitimate work purposes; **no illegal content/activity**.
- Do not install unapproved software or browser extensions.
- Do not bypass security controls, monitoring, or content filters.
- Personal cloud/email accounts must **not** be used for Organization data.
- Report suspected phishing, data loss, or malware **immediately**.

All users sign **Annex A – AUP Acknowledgement** on onboarding and annually.

---

6) Identity, Access & Authentication (RBAC/MFA)

- **Least privilege** and **Role-Based Access Control (RBAC)** for all systems.
- **MFA** is required for email, VPN, admin, finance/HR, donor systems, and any external access.
- **Passwords:** length ≥ 12, unique per system, password manager recommended; avoid reuse; change if compromise suspected.

- **Joiner-Mover-Leaver (JML):** create/modify/disable accounts within **1 business day** of status change; quarterly **access reviews** by system owners.
- **Service accounts/API keys:** documented purpose, owner, expiry/rotation **≤ 90 days** where supported; no shared admin accounts.

---

7) Endpoint Security (Laptops, Desktops, Mobiles)

- **MDM/endpoint management** required for Organization-owned devices; enforce encryption, firewall, screen lock, and auto-update.
- **EDR/anti-malware** installed and active; alerts monitored.
- **Patching:** critical security updates **≤ 72 hours**; high **≤ 14 days**; others monthly.
- **BYOD:** allowed only with MDM enrolment and policy acceptance; Organization can remove corporate data remotely.
- **USB/media:** restricted; use encrypted media only with approval.

---

8) Network & Remote Access

- Use **firewalls** and secure configurations; segment networks (e.g., guest Wi-Fi separated).
- **VPN** or **Zero-Trust** remote access with MFA for internal resources.
- **Wi-Fi:** WPA2-Enterprise/WPA3; passwords rotated; no default credentials.
- Block known malicious sites; DNS filtering and email security gateways recommended.

---

9) Cloud & Application Security

- Prefer **SaaS** with strong security, compliance attestations, and **EU/EAA data hosting** where feasible.
- Enforce **SSO** and MFA; restrict admin roles; log activity.

- Maintain a **System Register** with owners, data categories, locations, and retention.
- **Change management:** document changes; test before production; maintain version control.
- For custom code, use **secure development** practices (code review, dependency scanning, secret scanning).

---

10) Email & Collaboration Security

- Implement **SPF, DKIM, and DMARC (quarantine/reject)**.
- Disable auto-forwarding to external accounts; restrict external sharing by default; time-limit shared links.
- Train users on **phishing and social engineering**; simulate tests periodically.
- Use approved messaging tools; avoid personal messengers for official data.

---

11) Logging, Monitoring & Alerting

- Log authentication events, admin actions, changes, and security events; protect logs from tampering.
- Retain key security logs **≥ 12 months** (see Records Schedule).
- Review alerts daily; investigate and escalate per **Data Breach Response Plan**.

---

12) Vulnerability Management & Testing

- **Quarterly vulnerability scans** of endpoints and cloud services; remediate per patch SLAs.
- **Annual** independent **penetration test** for critical systems or after major changes.
- Track findings in a **risk register** with owners and deadlines.

---

13) Backup & Recovery (Resilience)

- Define **RPO/RTO** targets (e.g., RPO ≤ 24h; RTO ≤ 48h) per system criticality.
- Follow **3-2-1** backup strategy where feasible; encrypt backups; **test restores quarterly**.
- Separate backup credentials; protect against ransomware (immutable snapshots if available).

---

14) Third-Party & Vendor Security

- Conduct **security due diligence** before onboarding (Annex G); ensure **DPAs** and security clauses (incident notification, audit rights, sub-processors).
- Maintain a **Vendor/Processor Register**; review high-risk vendors **annually**.
- For payment/PII processors, confirm transfer mechanisms (DPF/SCCs) and data location.

---

15) Physical Security

- Control access to offices/rooms with keys/badges; maintain visitor logs.
- Secure equipment (cable locks/safe storage); avoid leaving devices in cars; lock screens when away.
- Keep server/network gear in restricted areas.

---

16) Cryptography & Key Management

- Use modern protocols (**TLS 1.2+**) and approved algorithms (**AES-256**, **RSA-2048/EC**).
- Manage certificates and keys centrally; rotate regularly; no hard-coded secrets; store secrets in a **secure vault**.

---

17) Incident Response & Reporting

- Suspected incidents must be **reported immediately** to IT/DPO.
- Handle per **Data Breach Response Plan**: triage within 24h, assess risk, contain, notify supervisory authority **within 72h** if required, and inform affected individuals when high risk.

---

18) Remote Work & Travel

- Use VPN/SSO with MFA; avoid public/shared devices; use privacy screens in public; do not discuss sensitive matters in public spaces.
- Report loss/theft of devices immediately; enable remote wipe.

---

19) Media Handling & Secure Disposal

- Wipe or destroy storage media before disposal or reuse (certified tools/vendor).
- Shred paper records containing personal or confidential data.
- Keep **Certificates of Destruction** where vendors are used.

---

20) Awareness, Training & Culture

- Induction training and **refreshers every 24 months**; targeted modules for managers/finance/HR/IT.
- Regular awareness campaigns (phishing drills, posters, tips).
- Record attendance and completion.

---

21) Exceptions & Risk Acceptance

- Exceptions to this Policy require a **documented risk assessment**, compensating controls, approval by IT & Security Lead and ED, and a review date.

---

22) Compliance, Audit & Review

- Periodic audits of access, configurations, backups, and vendor controls.
- Annual review of this Policy or after major incidents/changes; report to the National Board.
- Non-compliance may result in disciplinary action up to **termination** and vendor sanctions.

Annexes (Standards & Templates)

Annex A — Acceptable Use Policy (AUP) Acknowledgement

“I have read and agree to comply with the IT & Cybersecurity Policy and AUP.”
Signature: _____ Name: _____ Role: _____ Date: _____

Annex B — Access Control & Password/MFA Standard

- RBAC mapping; minimum password length **12**; MFA coverage; session timeouts; quarterly access reviews; JML checklist.

Annex C — Endpoint Baseline & Patch SLAs

- Encryption on; firewall on; EDR active; screen lock 5 min; USB blocked by default; patching timelines (critical ≤72h; high ≤14d; others monthly).

Annex D — Backup & Restore Matrix

- System; data type; RPO; RTO; backup frequency; storage locations; test schedule; owner.

Annex E — Logging & Monitoring Standard

- Events to log; retention **≥ 12 months**; alert thresholds; review cadence; storage and tamper protection.

Annex F — Email Authentication & Anti-Phishing Checklist

- SPF, DKIM, DMARC policy/quarantine/reject; mailbox rule audit; phishing simulation cadence; report-phish button.

Annex G — Vendor Security Questionnaire & DPA Checklist

- Hosting location; encryption; access controls; incident history; subcontractors; certifications; breach notice SLA; SCC/DPF status.

Annex H — Change Request Template

- Change description; risk/impact; test/rollback; approvals; schedule; post-change review.

Annex I — Security Incident Report Form

- Reporter; date/time; system; description; suspected cause; data categories; actions taken; escalation; case ID.

Annex J — Remote Work & Travel Checklist

- VPN/MFA; updated OS; encrypted device; privacy screen; secure Wi-Fi; clean desk; emergency contacts.

Annex K — Asset & System Register Fields

- Asset ID; owner; location; classification; data categories; vendor; contract dates; backups; RPO/RTO; last review.

Chapter 4. Data Breach Response Plan

Policy owner: Executive Director / Data Protection Officer (DPO)
Related policies: Privacy Policy; Information Security/IT Policy; Records Management & Data Retention; Whistleblowing & Complaints; Code of Conduct; Conflict of Interest (COI); Procurement & Ethical Purchasing; Financial Policy; Fraud Response Plan; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI.

---

1) Purpose & Scope

This Plan defines the steps, roles, timelines, and templates for responding to personal data breaches and other information security incidents affecting the Organization, in line with the GDPR 72-hour requirement and Lithuanian law. It applies to all personnel, contractors, suppliers (processors), and partners handling our data in any format (digital/paper).

Relationship to other documents: GDPR & Data Protection Policy; Privacy Policy; Information Security/IT Policy; Records Management & Data

Retention; Whistleblowing & Complaints; Child Protection & SEA Policies; Fraud Response Plan.

---

2) Definitions

- **Personal data breach:** a security incident leading to **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,** personal data (GDPR Art. 4(12)).
- **Incident:** any event that compromises confidentiality, integrity, or availability of information or systems, whether or not personal data are involved.
- **High risk:** likely to result in significant harm to individuals (e.g., identity theft, financial loss, discrimination, reputational damage, physical risk).

---

3) Principles

- **Speed with care:** act quickly while preserving evidence.
- **Accountability:** document every step in the **Breach Register**.
- **Data protection by design & default:** minimise data exposure; share on a **need-to-know** basis only.
- **Confidentiality & non-retaliation:** protect reporters and involved staff acting in good faith.
- **Transparency:** notify authorities/data subjects **when required**, communicate clearly, and implement lessons learned.

---

4) Roles & Responsibilities

- **Executive Director (ED):** overall accountability; approves notifications to authority and data subjects; informs National Board; authorises public statements.
- **Data Protection Officer (DPO):** leads privacy assessment/notifications; maintains **Breach Register**; advises on DPIA/TIA; liaises with the supervisory authority.

- **IT & Security Lead:** leads **technical containment and forensics**; preserves logs; coordinates with vendors/hosting; restores services securely.
- **Ethics & Compliance Officer (ECO):** ensures non-retaliation; coordinates with Whistleblowing/Complaints; records cross-policy issues.
- **Records/Finance/HR Leads:** provide data inventories, retention context, and support subject identification/communications.
- **Communications Lead/Spokesperson:** prepares internal and external messages using approved templates.
- **Managers/Data Owners:** report incidents immediately; support scoping and mitigation.
- **All staff & partners: report immediately**; do not investigate on their own; do not "clean up" evidence.

---

5) Incident Intake & Triage (T0–T+24h)

5.1 Intake

- Reporter contacts **DPO/IT** or **privacy@** immediately; if child/SEA-related, also inform **DSL/CPO/PSEA FP**.
- Log in **Breach Register** (Annex A) and assign **Case ID**.

5.2 Immediate containment

- IT: isolate affected systems/accounts; block malicious access; revoke tokens/credentials; enable **MFA**; disable auto-deletions; take forensic snapshots.
- Physical: secure premises, devices, paper files.
- Finance: stop suspicious payments; inform bank if relevant.

5.3 Scoping (initial)

- What happened? When detected? Systems/data affected? Volume/types of personal data? Categories of data subjects? Encryption in place? Backups? Involvement of processors/vendors?

- Confirm whether **personal data** are involved. If not, manage under IT Incident Procedure, but still log.

---

6) Risk Assessment & Decision to Notify (T+24–48h)

Use **Annex B – Risk Assessment Matrix** to evaluate **likelihood and severity** of harm to individuals.

Notify the supervisory authority if the breach is **likely to result in a risk** to rights and freedoms.
Notify data subjects without undue delay if the risk is **high**.

Key factors: type/sensitivity of data (e.g., IDs, financial, health, children); volume; ease of identification; security measures (encryption/pseudonymisation); context of data subjects (vulnerable groups); potential consequences; risk mitigation already applied.

Decision and rationale are documented in the **Breach Register**. DPO drafts notifications; ED approves.

---

7) Notifications (Templates in Annexes)

- **Supervisory Authority (within 72 hours):** include nature of breach, categories/approx. number of data subjects and records, likely consequences, measures taken/proposed, DPO contact (Annex C).
- **Data Subjects (without undue delay when high risk):** plain language notice with what happened, what data, risks, actions taken, steps they should take, and our contact (Annex D).
- **Donors/Partners/Authorities (as applicable):** per contracts/law.
- **Public statement/FAQ** (if needed): pre-approved messaging to avoid confusion (Annex E).

If notification might seriously hinder an investigation or create disproportionate risk, consult DPO/ED/legal on **temporary delay** as allowed by law.

---

8) Containment, Eradication & Recovery

- Remove malicious artefacts; rotate keys/passwords; patch vulnerabilities; harden configurations.
- Restore from **clean backups**; validate integrity; monitor for recurrence.
- If vendor breach: require vendor **incident report**, evidence of containment, and remediation plan; consider suspension or replacement.

---

9) Evidence Handling & Forensics

- Maintain **Chain of Custody** (Annex F) for all evidence (logs, images, emails, devices).
- Do not alter timestamps or metadata; work on copies where feasible.
- Store evidence in a restricted, encrypted repository.

---

10) Common Scenarios — Quick Playbooks

- **Phishing/Account Compromise:** force logout; reset passwords; enable MFA; review mailbox rules; notify contacts if spoofed.
- **Email mis-send/CC error:** attempt recall; contact unintended recipients; request deletion; assess risk based on content; consider subject notification.
- **Lost/stolen device:** remote lock/wipe; assess encryption; notify if unencrypted data may be exposed.
- **Ransomware:** isolate network segments; disable shares; evaluate backups; **do not pay** without ED/legal decision; notify authority if personal data affected.
- **Website/server intrusion:** take offline if needed; rotate credentials; review logs; patch; notify users if data exposure likely.
- **Processor/vendor breach:** trigger contract clauses; coordinate notifications; review vendor security; consider debarment.

---

11) Post-Incident Review & Lessons Learned (T+14–30d)

Within **2–4 weeks** after closure, hold a review to:

- confirm root cause and control gaps;
- implement corrective actions (technical, organisational, training);
- update policies, DPIAs, and risk registers;
- brief the National Board;
- document the review in **Annex G – Post-Incident Review Report**.

---

12) Training, Testing & Awareness

- **Annual** breach response drill/table-top exercise; update this Plan accordingly.
- Induction and **24-month refreshers** for all staff; extra for IT/Comms/Managers.
- Phishing simulations; privacy/security tips; breach posters with contacts.

---

13) Records & Retention

- **Breach Register** with case ID, dates, description, decisions, notifications, outcomes.
- Retain breach files for **10 years** (or as legally/donor required).
- Ensure alignment with the **Data Retention Schedule** in GDPR & Privacy Policies.

Annexes (Templates)

Annex A — Breach Register Entry & Intake Form

- Reporter; date/time; channel; summary; systems/data; initial actions; assigned leads; case ID.

Annex B — Risk Assessment Matrix (Likelihood × Severity)

- Criteria and scoring table; threshold guidance for authority and data subject notifications.

Annex C — Supervisory Authority Notification Template (≤72h)

- Required GDPR fields; DPO contact; attachments list.

Annex D — Data Subject Notification Template

- Plain-language notice; recommended protective steps (e.g., password change, fraud alerts); FAQ.

Annex E — Public Statement & Q&A Template

- Key messages; media/press instructions; do’s & don’ts; spokesperson.

Annex F — Evidence Log & Chain of Custody

- Item ID; description; collected by; date/time; storage; transfers/signatures.

Annex G — Post-Incident Review Report

- Timeline; root cause; impact; remediation; lessons learned; policy updates; sign-offs.

Annex H — Lost/Stolen Device Checklist

- Asset details; encryption status; remote lock/wipe; accounts accessed; subject risk.

Annex I — Vendor/Processor Breach Notification Letter

- Contract references; incident summary; required actions and timelines; audit/cooperation rights.

Annex J — Ransomware Decision Guide

- Law enforcement contact; data exfiltration assessment; offline restore plan; payment decision framework; communications.

Chapter 5. Records Retention & Destruction Schedule

Policy owner: Executive Director / Records Manager & Data Protection Officer (DPO)
Related policies: GDPR & Data Protection Policy; Privacy Policy; Information Security/IT Policy; Financial Policy; Procurement & Ethical Purchasing; Code of Conduct; Conflict of Interest (COI); Whistleblowing &

Complaints; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI; Records Management Standard.

---

1) Purpose & Scope

This Schedule defines how long the Organization keeps each type of record, the trigger for retention, the record owner, the storage location, and the approved destruction method. It applies to all records (digital and paper) created or received by the Organization and by processors acting on our behalf.

---

2) Principles & Legal Framework

- **GDPR Art. 5(1)(e)** – storage limitation: keep personal data **no longer than necessary**; delete/anonymise when no longer needed.
- **Accuracy & integrity:** maintain reliable, complete records with appropriate security.
- **Lawful retention:** where law or donor rules require longer periods, those prevail.
- **Document holds:** this Schedule is suspended by any **Legal/Litigation Hold** until release.

---

3) Roles & Responsibilities

- **National Board:** approves this Schedule; receives annual assurance on compliance.
- **Executive Director (ED):** accountable for implementation and resources.
- **Records Manager (with DPO):** maintains this Schedule, trains staff, monitors compliance, issues **Legal Hold Notices**, and coordinates destruction.
- **IT & Security Lead:** implements storage, backup, access, and secure deletion tools.
- **Finance Manager/Chief Accountant (FM/CA):** ensures finance/grant retention (typically **10 years**) and audit trail.

- **HR/People & Culture Lead:** ensures HR retention and secure personnel files.
- **Safeguarding Leads (DSL/CPO & PSEA FP):** oversee retention of safeguarding case files.
- **Managers/Data Owners:** ensure correct filing and timely transfer/closure.
- **All staff & processors:** follow this Schedule; do not delete records subject to hold.

---

4) Legal/Litigation Hold (Suspension of Destruction)

When litigation/regulatory investigation is reasonably anticipated or active, the Records Manager/DPO issues a Legal Hold Notice (Annex B). Destruction of affected records must stop immediately until the hold is lifted in writing.

---

5) Master Retention Schedule (Summary)

Notes: Periods below are **minimum** retention. Where donor contracts, law, or risk require longer, adopt the longer period. “After closure” means after the project/case/contract end and final reporting. Unless specified, format is both **digital/paper**.

Category	**Record Type (examples)**	**Retention Period**	**Trigger/ Notes**	**Owner**	**Storage**	**Destruction Method**
Governance	Founding docs, statutes, registration certificates	**Permanent**	Historical value	ED/ Board Secretary	Secure archive	N/A
	Board minutes, resolutions, committees	**Permanent**	—	Board Secretary	Digital archive + offsite backup	N/A

	Policies & versions	7 years **after superseded**	Keep version history	Records Manager	DMS/ Share	Secure delete/shred
Strategy & Risk	Risk registers, audits, management letters	10 years	After closure	ED/ FM/CA	DMS	Secure delete/shred
Finance (core)	GL/ledgers, journals, vouchers, invoices, receipts	**10 years**	FY end	FM/CA	Accounting system + DMS	Secure delete/shred
	Bank statements/reconciliations, payment files	**10 years**	FY end	FM/CA	Secure drive	Secure delete/shred
	Asset register & disposals	Life of asset + **10 years**	After disposal	FM/CA	DMS	Secure delete/shred
	Payroll, tax, social contributions	**10 years**	FY end	HR/ FM/CA	HRIS/ Payroll	Secure delete/shred
Grants/ Donors	Grant agreements, budgets, reports	**10 years**	After project closure	FM/ CA/PM	DMS	Secure delete/shred
	Donation records, receipts (no full card data)	**10 years**	FY end	FM/CA	CRM/ DMS	Secure delete/shred
Procurement	Tenders, RFQs, bids,	**10 years**	After award/clo	Procurement	DMS	Secure delete/shr

	bid evaluations		sure	Lead		ed
	Contracts/ POs/SOWs	**10 years**	After expiry/termination	PL/ FM/CA	Contract register	Secure delete/shred
HR	Personnel files (employment, contracts, performance)	**10 years**	After separation	HR Lead	HRIS/ Secure files	Secure delete/shred
	Recruitment (unsuccessful candidates)	2 years	After campaign close	HR Lead	HRIS	Secure delete/shred
	Training & H&S records	5 years	After completion	HR/ H&S	DMS	Secure delete/shred
Safeguarding	Child protection/SEA case files (adults)	**10 years**	After case closure	DSL/ PSEA FP	Restricted vault	Secure delete/shred
	Child protection/SEA case files (children)	Until the later of **10 years after closure or** the child's **28th birthday**	Legal/risk	DSL/ PSEA FP	Restricted vault	Secure delete/shred
	Consent forms (images/media) – adults	5 years	After last use/withdrawal	Comms/DSL	DMS	Secure delete/shred
	Consent	Until **age**	Risk-base	Comm	DMS	Secure

	forms – children	**23 or** 5 years after last use (whichever later)	d	s/DSL		delete/shred
Programmes / Beneficiaries	Case files (non-safeguarding), attendance, referrals	5 years	After case/programme closure	Programme Lead	DMS	Secure delete/shred
IT & Security	System logs (auth/access), web logs	Up to **12 months**	Security operations	IT Lead	SIEM/ log store	Auto-purge/secure delete
	Backups	Per backup policy (e.g., daily/weekly/monthly cycles; max **12 months**)	Rotation	IT Lead	Backup system	Overwrite/destruct
	Data breach/incident files	**10 years**	After closure	DPO/ IT	Restricted vault	Secure delete/shred
Facilities & Assets	Lease agreements, utilities, maintenance	**10 years**	After expiry/closure	Ops Lead	DMS	Secure delete/shred
Insurance	Policies, endorsements	**10 years**	After expiry	FM/CA	DMS	Secure delete/shred
	Claims & incident files	**10 years**	After settlement/closure	FM/CA	DMS	Secure delete/shred
Communicat	Press	**Permanen**	Historical	Comm	DMS/	N/A

ions	releases, annual reports	**t**	value	s Lead	Websit e	
	Social media content/analytics	24 months	After capture	Comms Lead	Platform export	Secure delete
CCTV/Access Control (if used)	Video footage	30 days	Unless incident/ hold	IT/ Security	NVR	Auto-purge/secure delete
	Access control logs	12 months	Security operations	IT/ Security	System	Auto-purge

6) Storage, Security & Access

- Store records in approved document management systems (DMS) or secure shared drives with role-based access; avoid personal accounts/devices.
- Encryption for Confidential/Special Category records at rest and in transit.
- Maintain indexes/metadata for searchability and provenance.
- Paper archives: locked cabinets/rooms; fire-safe where appropriate.

---

7) Destruction & Disposal (Authorised)

- Destruction must be approved by the Records Manager and documented in the Destruction Log (Annex C).
- Methods: cross-cut shredding or certified destruction for paper; cryptographic erasure or secure wipe for digital; certified disposal for media/devices (Annex D).
- For joint-controller or processor contexts, ensure return or destruction clauses are executed and Certificates of Destruction obtained.

---

8) Digitisation & e-Records

- Scanned copies may replace paper if scans are complete, legible, tamper-evident, and stored in a trusted repository; record the scan date and quality check.
- Use approved e-signature tools; keep signature certificates with the record.
- Destroy superseded paper copies where legally allowed.

---

9) Backups & Business Continuity

- Backups follow the Backup Retention Standard (cycles, encryption, off-site copies).
- Destruction schedules apply to primary data; backups are purged via lifecycle policies; on legal hold, include backups in scope where feasible.

---

10) Monitoring, Training & Review

- Annual compliance checks and spot audits; report results to ED/National Board.
- Induction and refresher training every 24 months for relevant staff.
- This Schedule is reviewed at least annually or after significant changes to law, donor requirements, systems, or risk.

Annexes (Templates)

Annex A — Records Inventory Template

- Business area; record type; owner; format; location; retention; legal basis; sensitivity; disposal method; notes.

Annex B — Legal/Litigation Hold Notice

- Case ID; scope (systems/records); custodians; suspension of deletion; instructions; acknowledgement.

Annex C — Destruction Authorisation & Log

- Record category; date range; volume; method; approval signatures; vendor certificate reference.

Annex D — Certificate of Destruction (Vendor)

- Vendor details; items destroyed; method; date; chain of custody; authorised signatures.

Annex E — File-Naming & Indexing Standard

- Pattern (YYYY-MM-DD_Project_RecordType_Version); metadata fields; versioning rules.

Annex F — Digitisation Quality Checklist

- Legibility; completeness; scan settings; checksum; spot-check %; acceptance sign-off.

Chapter 6. Media, Storytelling & Image Consent Policy

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

---

1) Policy Statement & Purpose

This Policy sets standards for ethical storytelling and the lawful creation, use, and sharing of photographs, audio, and video (Media) featuring staff, volunteers, partners, beneficiaries, and members of the public. It ensures informed consent, dignity, Do No Harm, and compliance with GDPR and safeguarding duties.

Objectives: (a) protect the rights, safety, and privacy of individuals; (b) avoid exploitation or stereotyping; (c) obtain and manage valid consent; (d) securely store media and related personal data; (e) enable timely takedown/withdrawal.

---

2) Scope & Applicability

Applies to all who create, edit, manage, or publish Media for or on behalf of the Organization: employees, volunteers, interns, photographers, videographers, writers, translators, consultants, contractors, suppliers, implementing partners, and donors using our assets under agreement. Covers Media captured in any context (events, field work, office, online) and all channels (web, social, print, reports, donor materials, press).

---

3) Key Definitions (Plain Language)

- **Media:** photographs, audio recordings, video, livestreams, transcripts, quotes, case stories, and related metadata (location, captions).
- **Personal data:** any information that can identify a person (faces, voice, name, contact details, unique context).
- **Special category data:** sensitive data such as health, biometric identifiers, racial/ethnic origin, religion/belief, sexual orientation, political opinions.
- **Consent: freely given, specific, informed, and unambiguous** indication (written or recorded) by which a person agrees to the use of their image/voice/story for stated purposes; **withdrawable at any time** without negative consequences.
- **Child:** anyone under **18**; **guardian/parental consent** and **child assent** are required.
- **Vulnerable persons:** people who may face heightened risk (children; survivors of violence; refugees and migrants; people with disabilities; LGBTQ+ persons; persons facing persecution).

---

4) Principles

1. **Do No Harm & Dignity:** portray people respectfully; avoid sensationalism, stereotyping, or retraumatisation.
2. **Consent-first:** obtain valid consent **before capture** where feasible, or **before publication** at the latest (see §6). Consent is **not a condition** to receive services.

3. **Safety & Safeguarding:** assess risks (including reprisals), minimise identifiers, and consult **DSL/CPO** for child or SEA-related content.
4. **Privacy by design:** limit data collected; avoid unnecessary identifiers (e.g., exact addresses, faces if not needed).
5. **Accuracy & context:** captions and stories must be truthful; avoid composite quotes or misleading edits.
6. **Right to withdraw:** respect withdrawal requests and takedown timelines (§9).
7. **No commercial exploitation:** Media will not be sold or used for political endorsements or unrelated commercial advertising.

---

5) Roles & Responsibilities

- **Executive Director (ED):** overall accountability; approves high-risk publications; resolves escalations.
- **Communications Lead (Comms):** owns processes and templates; maintains **Media/Consent Register**; reviews content; trains staff; manages takedowns.
- **Data Protection Officer (DPO):** ensures GDPR/consent compliance; maintains ROPA entries; advises on DPIAs/TIAs where needed.
- **Designated Safeguarding Lead (DSL/CPO) & PSEA Focal Point:** review child/SEA content and high-risk cases; ensure safeguarding controls.
- **Programme & Country Leads:** validate context and accuracy; ensure community engagement and permissions.
- **Photographers/Videographers/Storytellers (internal/external):** follow this Policy; obtain consent using approved forms; secure raw files; hand over all assets and logs.
- **All personnel & partners:** report concerns and withdrawal requests promptly; use only approved assets and channels.

---

6) Consent Standards & Workflows

6.1 Adults (18+)

- Use **Annex A – Adult Media & Image Consent** (written) or **Annex D – Audio/Video Recorded Consent**.
- Consent must cover: identity of controller; purpose(s); channels; territories; retention; right to withdraw; whether names/locations will be used; third-party sharing (donors/press/partners).
- Offer options (tick-boxes) to restrict: **face shown / first name only / anonymised** (blur/obscure), **no social media**, **no third-party sharing**, **time-limited** use.

6.2 Children (<18)

- **Required: Guardian consent** (**Annex B**) **and** age-appropriate **child assent** (**Annex C**).
- Two-adult rule during capture; no one-on-one private sessions; adhere to Child Protection/SEA Policies.
- Default to **anonymisation** (no names, blurred faces, altered identifiers) unless a strong, documented best-interest case exists and DSL approves.

6.3 Public Events & Crowds

- Use **event signage** (**Annex G**) and registration notices.
- For close-ups or identifiable focus on a specific person, obtain **individual consent**.
- Provide opt-out mechanisms (e.g., distinct lanyards/areas).

6.4 Vulnerable Contexts

- For refugees, survivors, or at-risk groups: conduct a **Do No Harm risk assessment** (**Annex H**); normally anonymise; remove geotags; consider delayed publication or composite identities.

6.5 Third-Party & Partner Content

- Accept only if consent terms meet or exceed our standards; obtain **written assurance** and copies of consent where feasible; log source and licence.

---

7) Content Standards (Ethical Storytelling)

- **Dignity:** depict strengths and agency; avoid shock imagery.
- **Accuracy:** verify quotes and facts; label illustrative images as such.
- **Safety:** remove **EXIF/geolocation** metadata; avoid revealing precise locations or routines.
- **Cultural sensitivity:** respect customs and dress; secure translation review.
- **No inducements:** gifts must not be contingent on consent; reasonable refreshments/transport allowed.
- **Credits:** obtain consent for name credit; otherwise use generic "Participant" or pseudonym.

---

8) Storage, Security & Retention

- Store Media and consent forms in approved **DMS/asset libraries** with **role-based access**; encrypt where applicable; backup per IT Policy.
- Maintain a **Media/Consent Register** linking asset IDs to consent records, restrictions, and expiry.

Retention:

- **Consent forms (adults): 5 years after last use or withdrawal** (see Records Schedule).
- **Consent forms (children):** until **age 23** or **5 years after last use** (whichever later).
- **Media assets:** retain per consent scope or **max 5 years after last use**, unless archival value and explicit consent cover continued storage.

Securely delete Media and purge caches/CDNs when consent expires or is withdrawn, per **takedown SOP** (Annex J).

---

9) Withdrawal & Takedown (Rights)

- Individuals can withdraw consent at any time via email, phone, or the online form (Annex E).

- Acknowledge within 2 working days; remove from our website and social channels within 5 working days; stop new use immediately.
- For printed or third-party materials already in circulation, stop future use and inform partners; document limitations (e.g., already-distributed print runs).
- Log actions in the Media/Consent Register.

---

10) Intellectual Property & Licensing

- Unless otherwise agreed, creators providing services under contract grant the Organization a non-exclusive, worldwide, royalty-free licence to use the Media for organizational purposes as defined in consent.
- No transfer to third parties beyond the consent scope without additional permission.
- Prohibited: misleading edits, deepfakes, or synthetic audio/visuals that alter a person’s identity or context without explicit written consent.

---

11) AI/Automation & Biometrics

- Do not use identifiable Media of people to train AI models without explicit, informed consent covering that purpose.
- Do not enable face recognition or biometric categorisation in our tools.
- Generative edits must be labelled if material; avoid manipulations that could mislead or harm.

---

12) Approvals & Publication Workflow

- Use Annex I – Story & Asset Approval Checklist before publication (consent verified; risks assessed; captions reviewed; geo removed; licences clear).
- High-risk items require DSL/DPO review and ED sign-off.
- Keep a changelog of published assets/links for quick takedown.

---

13) Incidents & Complaints

- Handle suspected privacy/safety incidents per Data Breach Response Plan (72-hour assessment); coordinate with DPO and DSL.
- Complaints are logged via Whistleblowing & Complaints procedures; non-retaliation applies.

---

14) Training & Communication

- Induction for all staff/volunteers; annual refreshers for Comms/Programme teams and anyone capturing Media.
- Quick guides and posters for field work; pre-event briefings on signage and consent.

---

15) Non-Compliance & Sanctions

- Breaches may result in corrective actions, retraining, removal of publishing rights, disciplinary measures up to termination, and vendor/partner remedies.

Annexes (Templates & Checklists)

Annex A — Adult Media & Image Consent Form

- Controller; purpose/channels; territories; duration; restrictions; name/credit options; third-party sharing; withdrawal right; signatures.

Annex B — Parent/Guardian Consent for Child

- Child details; guardian relationship/ID; purpose; anonymisation default; assent required; signatures.

Annex C — Child Assent Form (Age-Appropriate)

- Simple language explanation; agree/decline options; right to change mind; signature/drawing.

Annex D — Recorded (Audio/Video) Consent Script

- Script covering controller, purpose, channels, duration, withdrawal, and restrictions.

Annex E — Consent Withdrawal & Takedown Request Form

- Requester details; asset(s) and link(s); reason (optional); preferred contact; acknowledgement.

Annex F — Shot Log & Metadata Template

- Asset ID; date/time; location (general); subjects/consent form IDs; restrictions; caption notes; photographer; storage path.

Annex G — Event Signage (Photography & Filming Notice)

- Short notice text; opt-out mechanism; contact at venue; link/QR to full Policy.

Annex H — Do No Harm & Risk Assessment (Story/Media)

- Risks (safety, stigma, legal); mitigation (anonymise, delay, composite); DSL/DPO review; decision.

Annex I — Story & Asset Publication Checklist

- Consent verified; captions accurate; EXIF/geo cleared; safeguarding reviewed; approvals; links logged.

Annex J — Takedown SOP

- Acknowledge ≤ 2 working days; remove web/social ≤ 5 working days; notify partners; purge caches; confirm to requester; log closure.

Chapter 7. Cookie Policy

Related policies: GDPR & Data Protection Policy; Privacy Policy; Information Security/IT Policy; Records Management & Data Retention; Code of Conduct; Procurement & Ethical Purchasing; Whistleblowing & Complaints; Child Protection & Safeguarding; SEA Prevention & Response; Non-Discrimination & DEI.

---

1) Purpose & Scope

This Cookie Policy explains how the Organization uses cookies and similar technologies (pixels, local storage, SDKs) on our websites and online services (including adliga.fund) and how you can control them. It applies to all users and visitors.

---

2) Controller & Contact

Controller: VšĮ Tarptautinis pilietinių iniciatyvų centras „Mūsų namai“ (Lithuania).
Privacy inbox: privacy@adliga.fund
DPO: *Name, phone, email*
For general data-protection information, see our **Privacy Policy**.

---

3) What Are Cookies?

Cookies are small text files placed on your device by a website. They can be first-party (set by our site) or third-party (set by another domain), and can be stored for a session or persist for a defined period. Similar technologies include pixels, local storage, and SDKs.

---

4) Categories & Purposes

We group cookies as follows (non-exhaustive):

- **Strictly Necessary:** enable core functions (security, network management, donation checkout, consent settings). These do **not** require consent.
- **Preferences/Functionality:** remember choices (language, region, accessibility).
- **Analytics/Performance:** measure use, improve content and performance (e.g., page views, load time).
- **Marketing/Advertising:** measure campaigns and show relevant messages (only if used).
- **Security/Anti-fraud:** detect abuse or fraud in forms or payments.

---

5) Legal Basis & Consent

- We set strictly necessary cookies under legitimate interests to operate the site.
- We set non-essential cookies only with your consent (ePrivacy/GDPR). You can withdraw or change consent at any time via the Cookie Manager (link in footer or banner).

Children: our donation and public sites are not directed to children; where programmes involve children, we apply our Safeguarding and Privacy Policies.

---

6) Cookie Banner & Preference Management

Our banner offers **"Accept all", "Reject all", and "Save preferences"** with granular toggles for categories. Non-essential cookies are **off by default** until you consent.

- Manage preferences anytime via **Cookie Manager**: */cookie-preferences* (update once configured).
- We keep a **consent log** (timestamp, categories, country/IP, version) and request **re-consent at least every 12 months** or when the vendor set changes.
- We honour **Global Privacy Control (GPC)** signals by treating them as an **opt-out for non-essential cookies**, where technically feasible.

---

7) Third-Party Cookies & Providers

Some features use third-party services that may set cookies when you interact with them (e.g., payment processors like Stripe/PayPal; donation plugins like GiveWP; analytics tools). These providers process data under their own privacy terms. See Annex B – Common Providers.

International transfers (e.g., to the United States) are managed per our GDPR & Data Protection Policy (DPF/SCCs, supplementary measures).

---

8) Managing Cookies in Your Browser

You can also control cookies via browser settings (block, delete, or clear site data). Instructions:

- Chrome/Edge/Brave: Settings → Privacy → Cookies and site data
- Firefox: Preferences → Privacy & Security → Cookies and Site Data
- Safari: Preferences → Privacy
  Blocking some cookies may affect site functionality (e.g., donation checkout).

---

9) Data Retention

Cookie lifetimes vary. We keep cookie-related data **only as long as necessary** for the purpose and to comply with law. See the **Cookie Inventory** in Annex A for durations.

---

10) Changes to this Policy

We may update this Policy. The **Updated** date above shows the latest version. Significant changes will be communicated via the banner or site notice.

---

11) Contact & Rights

You may **withdraw consent** at any time via the Cookie Manager. For other rights (access, deletion, objection), see our **Privacy Policy** or contact **privacy@adliga.fund**.

Annexes

Annex A — Cookie Inventory (to complete and maintain)

Name	Provider	Category	Purpose	Duration	Type (1st/3rd)	Link to provider privacy
e.g., __stripe_mid	Stripe	Strictly necessary / Securi	Prevent fraud during checkout	1 year	3rd	https://stripe.com/privacy

		ty				
e.g., __stripe_sid	Stripe	Strictly necessary / Security	Session ID for payments	Session	3rd	https://stripe.com/privacy
e.g., paypal*	PayPal	Strictly necessary	Enable PayPal donations	Session–2 years	3rd	https://www.paypal.com/webapps/mpp/ua/privacy-full
e.g., give_wp*	GiveWP	Functional	Donation flow preferences	1 year	1st	https://givewp.com/privacy-policy/
e.g., _ga	Analytics provider	Analytics	Page analytics (IP anonymised)	13 months	1st/3rd	*insert*
e.g., _gid	Analytics provider	Analytics	Session analytics	24 hours	1st/3rd	*insert*
e.g., marketing_tag	Ad/marketing provider	Marketing	Campaign measurement	up to 13 months	3rd	*insert*

Replace examples with your actual inventory; keep it up-to-date.

Annex B — Common Providers (examples)

- **Stripe** (payments): may set cookies to prevent fraud and enable checkout; see privacy terms at stripe.com/privacy.

- **PayPal** (payments): may set cookies to enable payment and fraud prevention; see paypal.com/privacy.
- **GiveWP** (donation plugin): may store preferences to manage donation forms; see givewp.com/privacy-policy.
- **Analytics provider** (e.g., GA4, Matomo): used only with consent; configure IP anonymisation and data retention; see provider's privacy terms.

Annex C — Consent Log Fields

- User ID/anonymous token; timestamp; categories consented; device/browser; country/IP; banner version; CMP vendor list version; withdrawal timestamp.

Annex D — Banner Text (Short Notice)

We use cookies to run the site, secure donations, and improve content. Click Accept all to consent to analytics/marketing, Reject all to use only necessary cookies, or Save preferences to choose categories. You can change your choices anytime in Cookie Manager.

Annex E — Testing Checklist (Release/Changes)

- Non-essential cookies blocked prior to consent; category toggles work; GPC respected; consent stored and retrievable; re-consent after 12 months; links to Privacy/Cookie Policies present; withdrawal deletes/blocks tokens.