NOVEMBER 5, 2025

# UNIFIED MEL FRAMEWORK

*INTEGRATING MONITORING, EVALUATION, AND LEARNING SYSTEMS WITH VERIFICATION, ADAPTIVE MANAGEMENT, AND DATA GOVERNANCE.*

**CREATED BY**
EUSL AB
*Care to Change the World*

# Table of Contents

# Unified MEL Framework

## Chapter 1 — Logic Model and Theory of Change

**1.1 Purpose and scope.**

This Chapter establishes the foundational logic model and theory of change for all GSIA programs implemented under Flowhub Trio Plus, including those operating under Standard Custodianship or Hosted Ownership variants. It binds GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated vehicles, and participating Members or Hybrid RECs. The logic model provides a structured representation of inputs, activities, outputs, outcomes, and impacts, while the theory of change articulates the causal pathways and assumptions that underpin program success. Both instruments are mandatory for program approval and domestication readiness.

**1.2 Constitutional placement and prevalence.**

The MEL framework is integral to the GSIA Charter's public-interest mandate and is expressly referenced in the PPA and SLA. Where inconsistencies arise between MEL provisions and private instruments, the Charter and this Document prevail, subject only to mandatory national public law. MEL obligations cannot be waived or diluted by side letters or special conditions except through reasoned resolution of the GSIA SCE oversight organ and publication of such resolution.

**1.3 Logic model architecture.**

The GSIA logic model is structured as follows:

- **Inputs:** Financial resources (subscriptions, governance commission, buffers), technical expertise, fiduciary systems, ESG safeguards, and digital trust infrastructure.
- **Activities:** Governance-as-a-service functions (policy translation, fiduciary custody, procurement integrity), delivery orchestration (milestone gating, vendor management), capacity-building (shadow-to-lead domestication), and enabling functions (risk, continuity, data protection).
- **Outputs:** Ring-fenced fiduciary structures operational; procurement plans executed; milestones delivered; domestication benchmarks achieved progressively; publication dashboards issued; grievance mechanisms active.
- **Outcomes:** Strengthened institutional capacity; improved fiduciary integrity; enhanced transparency and accountability; inclusive and ESG-compliant service delivery; readiness for national ownership.
- **Impact:** Sustainable governance systems embedded in national institutions; resilience against fiduciary and ESG risks; equitable access to services; long-term social and economic benefits aligned with Agenda for Social Equity 2074.

**1.4 Theory of change narrative.**

The theory of change rests on the premise that temporary, benchmarked custodianship under Flowhub accelerates institutional maturity by combining fiduciary integrity, transparency, and capacity-building with enforceable ESG safeguards. If GSIA provides governance-as-a-service under ring-fenced conditions, and if Members progressively assume operational roles through structured domestication gates, then fiduciary risk declines, procurement integrity improves, and public confidence rises, leading to sustainable national ownership and inclusive development outcomes. Assumptions include:

(a) political will to adopt and enforce fiduciary and ESG standards;
(b) availability of qualified counterpart staff for shadowing and transition;
(c) legal frameworks permitting ring-fencing and publication;
(d) donor and DFI alignment with GSIA governance doctrine; and
(e) continuity of operations during external shocks through stress-tested protocols.

**1.5 Risk and mitigation logic.**
Risks to the theory of change include political instability, legal reversals, fiduciary breaches, safeguarding failures, and data-protection lapses. Mitigation measures embedded in the MEL framework include KRIs linked to escalation protocols (Document 17), independent assurance (Document 09), and adaptive management loops (Chapter 4 herein). Residual risks are disclosed in MEL dashboards and reviewed by the Audit and Risk Committee.

**1.6 Domestication linkage.**
The logic model and theory of change are operationalised through domestication benchmarks embedded in the PPA and SLA. MEL indicators track readiness gates (functional shadowing, dual-key operations, lead-role transition, system handover, legal localisation) and inform readiness certification decisions by GSIA SCE oversight organs.

**1.7 Publication and transparency.**
The logic model and theory of change for each program are published in summary form, with lawful redactions for sensitive data, as part of the MEL portal. Updates reflecting adaptive management decisions are time-stamped and archived in tamper-evident repositories.

## Chapter 2 — Indicators and Baselines

**2.1 Purpose and scope.**
This Chapter codifies the indicator architecture and baseline establishment protocols for GSIA programs. Indicators measure progress across fiduciary integrity, procurement transparency, ESG compliance, gender and inclusion, digital trust, grievance handling, and domestication readiness. Baselines provide reference points for KPI targets and verification standards embedded in SLAs and Implementation Agreements.

**2.2 Indicator taxonomy.**
Indicators are classified into six mandatory domains:
(a) **Fiduciary integrity:** e.g., percentage of transactions with dual approvals; reconciliation timeliness; exception rates; compliance with ring-fencing (zero unauthorised inter-project transfers).
(b) **Procurement integrity:** e.g., share of competitive awards; protest resolution timeliness; conflict-of-interest disclosure compliance; publication of award notices within SLA timelines.
(c) **ESG and inclusion:** e.g., implementation of environmental and social management plans; safeguarding incident rates; participation of women-owned and inclusive enterprises; accessibility compliance for infrastructure and digital services.
(d) **Digital trust and data protection:** e.g., IAM recertification rates; SIEM alert closure times; DPIA completion for high-risk processing; breach notification timeliness.
(e) **Grievance redress:** e.g., average resolution time; percentage of grievances closed within SLA timelines; escalation rates; complainant satisfaction scores (aggregated and anonymised).
(f) **Domestication readiness:** e.g., number of functions transitioned to Authority lead; competency certification rates; system handover milestones achieved; legal localisation progress.

**2.3 Indicator characteristics.**
Indicators must be:

- **Specific:** Clearly defined with scope and unit of measure.
- **Measurable:** Quantifiable or verifiable through documented evidence.
- **Achievable:** Realistic given resources and context.
- **Relevant:** Linked to control objectives and theory of change.
- **Time-bound:** Associated with defined reporting periods and domestication gates.

**2.4 Baseline establishment.**
Baselines are established through diagnostic assessments at program inception, using validated tools and sampling protocols. Fiduciary baselines derive from PFM maturity assessments; procurement baselines from historical award patterns; ESG baselines from environmental and social screening; inclusion baselines from gender and accessibility analyses; digital trust baselines from IAM and SIEM posture reviews; grievance baselines from existing complaint mechanisms; domestication baselines from institutional capacity diagnostics. Baseline reports are archived and summarised for publication with lawful redactions.

**2.5 Target setting and tiering.**
Targets are set in consultation with the Authority and GSIA oversight organs, calibrated to risk and capacity. Tiered performance bands (e.g., Tier A: on-target or better; Tier B: within tolerance; Tier C: below tolerance) are defined for each indicator, with remedies linked to SLA provisions. Targets for domestication indicators align with readiness gates and certification criteria.

**2.6 Verification sources.**
Indicators rely on primary records, immutable logs, reconciliations, acceptance certificates, audit findings, and independent verification where mandated. Data lineage from source to dashboard is documented to evidentiary standards. Verification protocols are detailed in Chapter 3.

**2.7 Publication and dashboards.**
Indicator definitions, baselines, targets, and quarterly performance dashboards are published in accordance with the transparency doctrine, with privacy-preserving techniques applied to sensitive data. Exceptions require reasoned, time-limited resolutions recorded and disclosed.

**2.8 Interfaces.**
This Chapter interfaces with Chapter 3 (Verification and Reporting Protocols), Chapter 4 (Adaptive Management), and Document 12 (Data Governance for MEL). Nothing herein permits dilution of fiduciary, ESG, or publication obligations.

# Chapter 3 — Verification and Reporting Protocols

**3.1 Purpose and binding character.**
This Chapter codifies the verification standards and reporting protocols that govern measurement, assurance, and disclosure across all GSIA programs implemented under Flowhub Trio Plus. It binds GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated vehicles, Members and Hybrid RECs in their roles as competent authorities, and all contracted vendors and validators operating within ring-fenced perimeters. Verification and reporting are treated as non-derogable control functions aligned to fiduciary integrity, ESG safeguards, and domestication gates; any time-limited departure requires a

reasoned resolution of the competent GSIA SCE oversight organ and recorded publication with lawful redaction.

**3.2 Verification doctrine and evidentiary standards.**
Verification rests upon the primacy of contemporaneous, primary records; immutable logs; and reproducible methods. Measurements of indicators and KPIs shall be supported by source documents, machine-generated event logs, acceptance certificates, reconciliation artefacts, and, where applicable, independent attestations. All evidence is retained in tamper-evident repositories with chain-of-custody records sufficient to maintain probative value before internal and external assurance functions and, if necessary, dispute-resolution fora. Derived metrics shall preserve lineage to source data and transformation logic.

**3.3 Layers of assurance.**
Assurance is structured across three mandatory layers. First-line management controls generate measurements and compile reports in accordance with this Framework and the SLA. Second-line compliance functions monitor adherence, test samples, and validate closure of corrective actions. Third-line Internal Audit provides independent assurance over design and operating effectiveness, coordinates reliance on external validators, and reports to the Audit and Risk Committee in accordance with Document 05. External independent validation, where mandated by program risk or materiality, is commissioned under Document 09 and does not displace internal accountability.

**3.4 Measurement protocols.**
Each indicator defined under Chapter 2 shall have an approved Measurement Protocol specifying scope, unit of measure, calculation methodology, acceptable error margins, evidence sources, sampling frames where relevant, data-quality checks, and verification steps. Protocols are adopted by reasoned memorandum, version-controlled, and cross-referenced in the SLA KPI Schedule. Amendments are permitted where methods improve reliability or reduce burden without weakening control strength; amendments are recorded with effective dates and applied prospectively unless otherwise justified.

**3.5 Data collection and quality controls.**
Data collection is performed by designated roles identified in the authority matrix. Quality controls include completeness checks, reasonableness tests, variance analysis against baselines and prior periods, and reconciliation to financial, procurement, and operational ledgers. Where automated extraction is used, interface specifications, transformation logic, and validation routines are documented and tested. Manual adjustments are exceptional, justified by written note, dual-approved, and flagged for review by compliance and Internal Audit.

**3.6 Independent verification.**
Indicators associated with fiduciary integrity, procurement integrity, ESG high-risk categories, safeguarding, or domestication readiness gates shall, where so classified, be subject to independent verification by qualified personnel not involved in delivery or by third-party validators. Verification criteria and evidence requirements are defined in advance, and conclusions are issued in written form stating scope, methods, limitations, and findings. Disagreements between management and verifiers are recorded and escalated to oversight committees with a reasoned recommendation.

**3.7 Frequency and cadence.**
At minimum, monthly reports cover cash and commitments, exception summaries, critical incident logs, and progress on time-sensitive indicators. Quarterly reports include ring-fenced financial

statements, KPI dashboards across all domains, procurement summaries, ESG performance reports, and compliance status against corrective actions. Semi-annual reports incorporate outcome-level narratives and progress toward domestication gates. Annual reports provide a comprehensive performance summary, including lessons learned and readiness assessments. Cadence is calendarised in the SLA and shall not be unilaterally altered.

**3.8 Reporting structure and minimum content.**
Reports adhere to a standard structure: scope and period covered; indicator table with baselines, targets, and actuals; analysis of variance with causes; corrective and preventive actions with owners and timelines; data-quality notes; and an attestation by the responsible officer and countersignature by the beneficiary authority where required by threshold. Public-facing versions follow the transparency doctrine, with privacy-preserving redactions where lawful and necessary.

**3.9 Escalation and exception handling.**
Material deviations from targets, breach of service levels, or integrity flags trigger escalation under the SLA. Exception reports state the condition, criteria, cause, effect, and risk, together with a corrective action plan and agreed verification of closure. Repeated or systemic exceptions are elevated to the Audit and Risk Committee and, where linked to procurement integrity or ethics, to the Procurement and Integrity Committee and the Ethics, Conflicts and Investigations Committee.

**3.10 Interfaces with fiduciary, ESG, and digital-trust controls.**
Verification and reporting are integrated with fiduciary controls (Document 06, Chapter 5), ESG safeguards (Document 06, Chapters 1–2), anti-corruption protocols (Document 06, Chapter 3), grievance redress (Document 06, Chapter 4), and digital-trust requirements (Document 12 and Document 03, Chapter 5). Identity and access controls ensure only authorised personnel generate or approve reports. Immutable logs record report generation and approval timestamps and identities.

**3.11 Publication obligations.**
KPI dashboards, procurement summaries, ring-fenced financial statements, audit and verification summaries, and domestication progress reports shall be published according to a schedule annexed to the SLA. Time-limited delays or redactions must be justified by legal basis or safeguarding concerns, approved by reasoned resolution, and subject to periodic review. Public repositories maintain version history and integrity hashes for each published artefact.

**3.12 Readiness evidence for domestication gates.**
Gate reviews rely on a consolidated verification dossier comprising KPI histories, control-maturity assessments, competency certifications, independent verification reports, and legal-localisation checklists. Dossiers are assembled by GSIA AB, co-signed by the beneficiary authority, and presented to the Programs and Domestication Committee for recommendation to the oversight organ empowered to certify readiness.

**3.13 Record retention and legal holds.**
All verification artefacts and reports are retained per the records schedule and legal-hold procedures. Upon notice of investigation, dispute, or evaluation, disposition is suspended for affected records. Chain-of-custody for exported data and reports is maintained to evidentiary standards, including integrity hashes and access logs.

**3.14 Corrective action verification and closure.**
Corrective action plans include specific remedial steps, owners, due dates, and success criteria. Closure is verified by evidence review and, for significant findings, by Internal Audit or an independent validator.

Closed actions are tracked and reported; re-openings require a reasoned justification and a new timeline.

## Chapter 4 — Adaptive Management and Learning Loops

**4.1 Purpose and principle.**
Adaptive management ensures that evidence generated through verification and reporting leads to timely, reasoned adjustments in design, implementation, and domestication pathways without weakening fiduciary, ESG, or publication controls. Learning loops are institutionalised as a mandatory governance function rather than discretionary practice, with decisions recorded, justified, and published in accordance with transparency rules.

**4.2 Architecture of learning loops.**
Learning operates across three nested loops. The operational loop addresses short-cycle adjustments to procurement plans, sequencing, and resource allocations within established controls. The tactical loop addresses quarterly recalibrations to service levels, indicator targets, and domestication pacing based on performance and contextual shifts. The strategic loop addresses annual or milestone-based re-designs, including re-scoping, re-phasing, or technology choices, subject to board-level approval and publication.

**4.3 Triggers for adaptation.**
Adaptation is triggered by statistically significant deviations from targets; repeated exceptions; incident post-mortems; independent evaluation findings; changes in risk posture (including political, legal, or macroeconomic shifts); safeguarding or inclusion concerns; and technological obsolescence or opportunity. Triggers and thresholds are defined in the SLA and documented in the Monitoring Plan.

**4.4 Decision-rights and safeguards.**
Operational adaptations within the perimeter are approved under the authority matrix, do not alter ring-fencing or domestication covenants, and are recorded in change-control logs. Tactical adaptations that recalibrate KPIs or service levels require approval by the competent committee(s) and are implemented through reasoned addenda to the SLA. Strategic adaptations that affect scope, budget structure, domestication gates, or Hosted Ownership covenants require oversight organ resolution and, where applicable, amendments to the PPA, Leasing Instrument, or Implementation Agreement. In all cases, adaptations may not dilute controls or publication duties.

**4.5 Hypothesis management and documentation.**
Each material adaptation is framed as a testable hypothesis specifying the change, expected effect, time horizon, indicators to observe, and success criteria. A pre-registered Adaptation Note records the baseline, rationale, counterfactual options considered, and risk assessment. Upon review, outcomes are compared to expectations, and the hypothesis is confirmed, refined, or rejected with reasons. Notes are archived and summarised for publication.

**4.6 Feedback integration from GRMs and stakeholders.**
Grievance redress data and structured stakeholder feedback are treated as primary inputs to learning. Periodic analyses identify systemic issues (e.g., accessibility barriers, vendor performance patterns, safeguarding risks) and propose remedial adaptations. Where consent allows, anonymised case insights inform design changes and contract conditions. Feedback mechanisms remain accessible and non-retaliatory throughout.

**4.7 Linkage to risk management and stress testing.**
Adaptive decisions incorporate outputs from the enterprise and programmatic risk frameworks (Document 17) and financial stress-testing and continuity planning (Document 10). Where adaptations increase exposure or alter risk profile, KRIs, buffers, and continuity protocols are adjusted accordingly and approved under the proper authority.

**4.8 Capacity-building and domestication alignment.**
Learning loops explicitly support the shadow-to-lead progression. Adaptations include revised training curricula, adjusted thresholds for beneficiary countersignature, and re-sequencing of system administration transfers. Competency gains are evidenced through certifications and observed performance, and are used to unlock domestication gates under Chapter 3 of this Document and the SLA.

**4.9 Technology and data improvements.**
Where data quality or timeliness impedes learning, adaptations may include automation of data capture, enhancement of logging and SIEM rules, introduction of privacy-preserving analytics, or refinement of ETL pipelines. Such changes are governed by documented change-control, tested for integrity impact, and approved under the authority matrix. No adaptation may circumvent data-protection obligations.

**4.10 Publication of adaptations and lessons.**
Material adaptations and their rationales are summarised in quarterly public dashboards. Annual learning reports synthesise key lessons, validate or retire hypotheses, and state implications for future cycles and for replication across programs. Time-limited redactions are permitted only where legally required or necessary to protect safeguarding or security.

**4.11 Evaluation interface and course-correction.**
Findings from independent evaluations (Document 09) are integrated into strategic learning loops. Management must provide time-bound response plans to address recommendations, and progress is tracked and disclosed. Where evaluations identify material design flaws or context changes, course-corrections are proposed to boards with explicit consideration of costs, benefits, and risk implications.

**4.12 Records and retention.**
Adaptation Notes, change-control logs, committee decisions, and published summaries are maintained in tamper-evident repositories under the records schedule. Legal holds apply where adaptations relate to incidents under investigation or pending disputes.

**4.13 Non-regression rule.**
Adaptive management shall not be used to relax fiduciary controls, publication duties, ESG safeguards, or reversion covenants. Any proposed adaptation that would reduce control strength is inadmissible absent an express, time-limited waiver by the competent oversight organ supported by a risk impact assessment and public justification; such waivers expire automatically unless renewed by reasoned resolution.

**4.14 Replicability and scale-out.**
Positive adaptations with demonstrable effect become candidates for standardisation across the GSIA corpus. The Secretariat maintains a repository of validated patterns and decision templates, which are proposed for incorporation into Manuals, templates, or standard clauses at the next scheduled revision cycle, subject to oversight approval and publication.

# Chapter 5 — Independent Evaluation Standards

**5.1 Purpose and binding character.**
This Chapter codifies the mandatory standards for independent evaluations commissioned within the GSIA institutional perimeter. It binds GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated vehicles, Members and Hybrid RECs acting as competent authorities, and any external evaluators, validators, or peer reviewers engaged under Flowhub Trio Plus. Independence is a non-derogable requirement; evaluation design, execution, and disclosure shall be insulated from delivery management influence and shall be preserved through instrumented safeguards.

**5.2 Constitutional placement and prevalence.**
Independent evaluations form part of the public-interest mandate established by the Charter and are referenced in the PPA and SLA. Where inconsistencies arise between any private instrument and this Chapter, the Charter and this Chapter prevail, subject only to mandatory national public law. Side letters shall not dilute independence, access, publication, or remedies prescribed herein.

**5.3 Evaluation typology and triggers.**
Evaluations comprise, at minimum: (i) formative and design-stage evaluations where material public value or risk is at stake; (ii) mid-term process and performance evaluations for programs exceeding one year in duration or materiality thresholds; (iii) end-term outcome and cost-effectiveness evaluations; and, where feasible and proportionate, (iv) impact evaluations using quasi-experimental or equivalent credible counterfactual methods. Triggers include scale, fiduciary or ESG risk class, domestication gates, persistent KPI variance, and incident patterns requiring systemic review.

**5.4 Independence and conflict safeguards.**
Evaluators shall be institutionally and functionally independent of GSIA AB delivery lines, of vendors within the perimeter, and of the competent authority's implementing units. Procurement of evaluators is conducted competitively and administered by a unit outside the delivery chain, under the Procurement and Integrity Committee's oversight. Conflict-of-interest declarations are mandatory for evaluators and their key personnel; recusals or disqualifications apply where conflicts are actual or perceived and cannot be effectively mitigated. Remuneration may not be contingent on positive findings or programme continuation.

**5.5 Terms of reference and protocols.**
Each evaluation proceeds under a written Terms of Reference (ToR) adopted by reasoned memorandum and published in summary. ToR shall specify scope, evaluation questions, theory of change to be tested, methods and limitations, data sources and access requirements, sampling frames, ethical and safeguarding protocols, analysis plans, deliverables, timelines, publication expectations, and requirements for management responses. Amendments to ToR are reasoned, recorded, and do not dilute independence or access.

**5.6 Methods and evidentiary standards.**
Methods shall be fit-for-purpose, rigorous, and replicable, and may include mixed methods combining quantitative analysis (including quasi-experimental designs, matched controls, interrupted time-series, or synthetic controls where feasible) and qualitative inquiry (key informant interviews, focus groups, process tracing, realist evaluation). Cost-effectiveness and value-for-money analysis are conducted where material, with explicit assumptions and sensitivity analysis. All findings shall rest upon verifiable evidence preserved in tamper-evident repositories with chain-of-custody, preserving data lineage from source to inference.

**5.7 Ethical, safeguarding, and data-protection considerations.**
Evaluations involving human participants adhere to ethical standards of informed consent, harm minimisation, and confidentiality, and to safeguarding obligations for vulnerable persons. Where required, institutional ethics approvals are obtained. Personal data processing conforms to the Data Protection and Digital Trust Policy and the DPA; privacy-preserving techniques are applied to publication outputs.

**5.8 Access, cooperation, and non-interference.**
Evaluators receive timely access to records, sites, systems, personnel, and vendors necessary to perform their mandate, subject to lawful constraints and data-protection safeguards. GSIA AB and competent authorities shall cooperate fully and refrain from interference. Non-cooperation or obstruction constitutes a material breach subject to remedies under the SLA and the Sanctions Grid.

**5.9 Quality assurance and peer review.**
Evaluation plans and draft reports undergo quality assurance by an independent methodologist or panel. For high-materiality evaluations, blind peer review is commissioned through the External Validation and Peer Review Protocol (Document 09). Methodological critiques and author responses are archived and, where feasible, summarised for publication.

**5.10 Findings, ratings, and management response.**
Reports present findings, conclusions, and recommendations with explicit linkage to evidence and the theory of change. Where rating scales are used (e.g., relevance, effectiveness, efficiency, sustainability, equity), scales and criteria are pre-declared. Management prepares a time-bound response plan with specific actions, owners, and timelines; responses are reviewed by oversight committees, integrated into adaptive management loops, and tracked to closure.

**5.11 Publication and transparency.**
Final reports, executive summaries, data dictionaries, and codebooks are published with lawful redactions. Where evaluators rely on confidential or sensitive data, anonymised extracts or aggregated results are published to preserve transparency without violating legal or safeguarding obligations. Publication delays require a reasoned, time-limited exception approved by the oversight organ and recorded.

**5.12 Timing and calendaring.**
Evaluation calendars are established at program outset and synchronised with domestication gates to maximise decision utility. Mid-term evaluations precede critical resourcing or design decisions; end-term evaluations precede domestication certification or scale-out decisions. Deviations from calendars require reasoned justification and oversight approval.

**5.13 Use and non-regression.**
Evaluation findings shall inform adaptations, investment decisions, and domestication pacing. Adaptations shall not reduce the strength of fiduciary, ESG, data-protection, or publication controls (non-regression). Where findings recommend dilution of controls, they are inadmissible absent an express waiver under strict conditions and public justification.

**5.14 Records and survivals.**
All evaluation artefacts—ToR, instruments, datasets (as lawfully sharable), analysis scripts, peer reviews, management responses, and closure evidence—are retained per the records schedule and legal holds. Survivals include audit access, confidentiality, and publication rights.

# Chapter 6 — Data Governance for MEL

**6.1 Purpose and scope.**

This Chapter establishes the data-governance architecture for Monitoring, Evaluation, and Learning (MEL) across all GSIA programs. It binds GSIA entities, Members and Hybrid RECs acting as competent authorities, vendors, processors, and evaluators. It prescribes roles, lawful bases, data standards, stewardship, quality controls, security, publication, and domestication benchmarks specific to MEL data, without derogating from the Data Protection and Digital Trust Policy or the DPA.

**6.2 Roles and allocation of responsibilities.**

Unless otherwise agreed in the DPA: the competent authority is controller for MEL personal data; GSIA AB is processor; independent evaluators are sub-processors or separate controllers only where they determine purposes independently under written arrangement. The Secretariat maintains the MEL data catalogue and metadata registry; the Compliance function monitors adherence; Internal Audit provides independent assurance. These allocations are recorded in instrument annexes and do not shift under Hosted Ownership.

**6.3 Lawful basis, minimisation, and fairness.**

MEL data collection and processing shall be necessary, proportionate, and grounded in a lawful basis (public task, legal obligation, legitimate interests where applicable, or explicit consent where required). Only data strictly necessary for indicators, verification, and evaluation are collected; sensitive data require heightened protections and explicit legal basis. Fair processing notices are issued in accessible form.

**6.4 Data architecture and standards.**

A common MEL data model is adopted, comprising master data (programs, perimeters, vendors, sites), reference data (indicator definitions, units, rating scales), and transactional data (observations, events, logs, reconciliations). Data elements carry unique identifiers, versioned metadata, provenance tags, and integrity hashes. Taxonomies and code lists are maintained centrally and referenced in the SLA KPI Schedule and the Evaluation ToR.

**6.5 Data quality and lineage.**

Data quality dimensions—completeness, accuracy, timeliness, consistency, validity, and uniqueness—are defined with thresholds and tests. Lineage from source systems to dashboards and reports is documented in data-flow maps and transformation specifications, preserved in tamper-evident repositories, and audited periodically. Manual overrides are exceptional, dual-approved, and flagged for review.

**6.6 Access control, logging, and security.**

Role-based access with least-privilege is enforced. Privileged access is just-in-time, dual-controlled, and fully logged. Logs are immutable, time-stamped, and retained to evidentiary standards. Encryption is applied in transit and at rest; key management follows dual-custody principles. Segregation between development, test, and production is maintained; test data are masked or synthesised.

**6.7 Disaggregation, privacy, and publication.**

Disaggregation for equity (e.g., gender, age bands, disability status where lawfully collected) is pursued to the minimum granularity necessary to detect disparities, balanced against re-identification risk. Publication uses aggregation thresholds, suppression rules, or privacy-enhancing techniques to prevent re-identification. Public MEL dashboards disclose definitions, baselines, targets, methods, and caveats.

**6.8 Data sharing, evaluators, and sub-processors.**
Data-sharing with evaluators and sub-processors is governed by written agreements specifying purpose limitation, security measures, onward-transfer controls, breach notification, and return/deletion at end of engagement. A public or Member-accessible register of MEL data-sharing arrangements and sub-processors is maintained and updated prior to engagement or material changes.

**6.9 Cross-border transfers and localisation.**
Cross-border transfers of MEL data occur only under lawful safeguards and as minimised by design. Where localisation is mandated, in-region processing and storage are implemented; remote support does not compromise localisation. Supervisory liaison arrangements for MEL datasets are documented and appended to the DPA.

**6.10 Reproducibility and open methods.**
To the extent lawful, anonymised datasets, data dictionaries, and analysis scripts for published evaluations are released to enable reproducibility. Where full release is not lawful or safe, synthetic datasets and method descriptions are provided. Code and method artefacts are version-controlled and integrity-anchored.

**6.11 MEL data retention and deletion.**
Retention schedules specify minimum and maximum periods for each MEL data category, balancing evidentiary needs, evaluation cycles, and minimisation. Upon domestication or termination, MEL data are transferred to the competent authority with integrity attestations; residual copies are securely deleted or irreversibly anonymised, save for records lawfully retained for audit or dispute resolution. Deletions are evidenced by destruction certificates.

**6.12 Incident response and data integrity.**
MEL data incidents—breaches, corruption, loss, or integrity compromise—are classified and handled under incident protocols aligned with the DPA and SLA. Responses include containment, root-cause analysis, restoration from trusted backups, and verification of integrity using hashes and logs. Material incidents are disclosed in public summaries with lawful redactions.

**6.13 Governance forums and decision rights.**
A MEL Data Governance Forum, chaired by the Data Protection and Digital Trust Committee with participation from the Programs and Domestication Committee and the Secretariat, approves indicator definitions, taxonomies, major data-model changes, and publication policies. Decisions are reasoned, recorded, and published in summary.

**6.14 Domestication benchmarks for MEL.**
Readiness for domestication includes demonstrated capacity to: administer the MEL data catalogue; maintain indicator definitions and taxonomies; operate data-quality controls and lineage documentation; enforce access controls and logging; execute DPIAs where required; manage evaluator data-sharing; and publish dashboards with privacy-preserving methods. Evidence is presented at domestication gates and reviewed for certification.

**6.15 Interfaces and non-regression.**
This Chapter interfaces with Verification and Reporting Protocols (Chapter 3), Adaptive Management (Chapter 4), Independent Evaluation Standards (Chapter 5), the Data Protection and Digital Trust Policy (Document 12), and instrument annexes to the PPA, SLA, IA, and DPA. No adaptation or instrument may reduce the strength of MEL data-governance safeguards without express, time-limited waiver supported by risk analysis and public justification.

**6.16 Records and survivals.**

MEL data catalogues, metadata registries, lineage artefacts, access logs, DPIAs, data-sharing registers, and publication artefacts are retained per the records schedule. Survivals include audit and access rights, confidentiality, and publication duties.