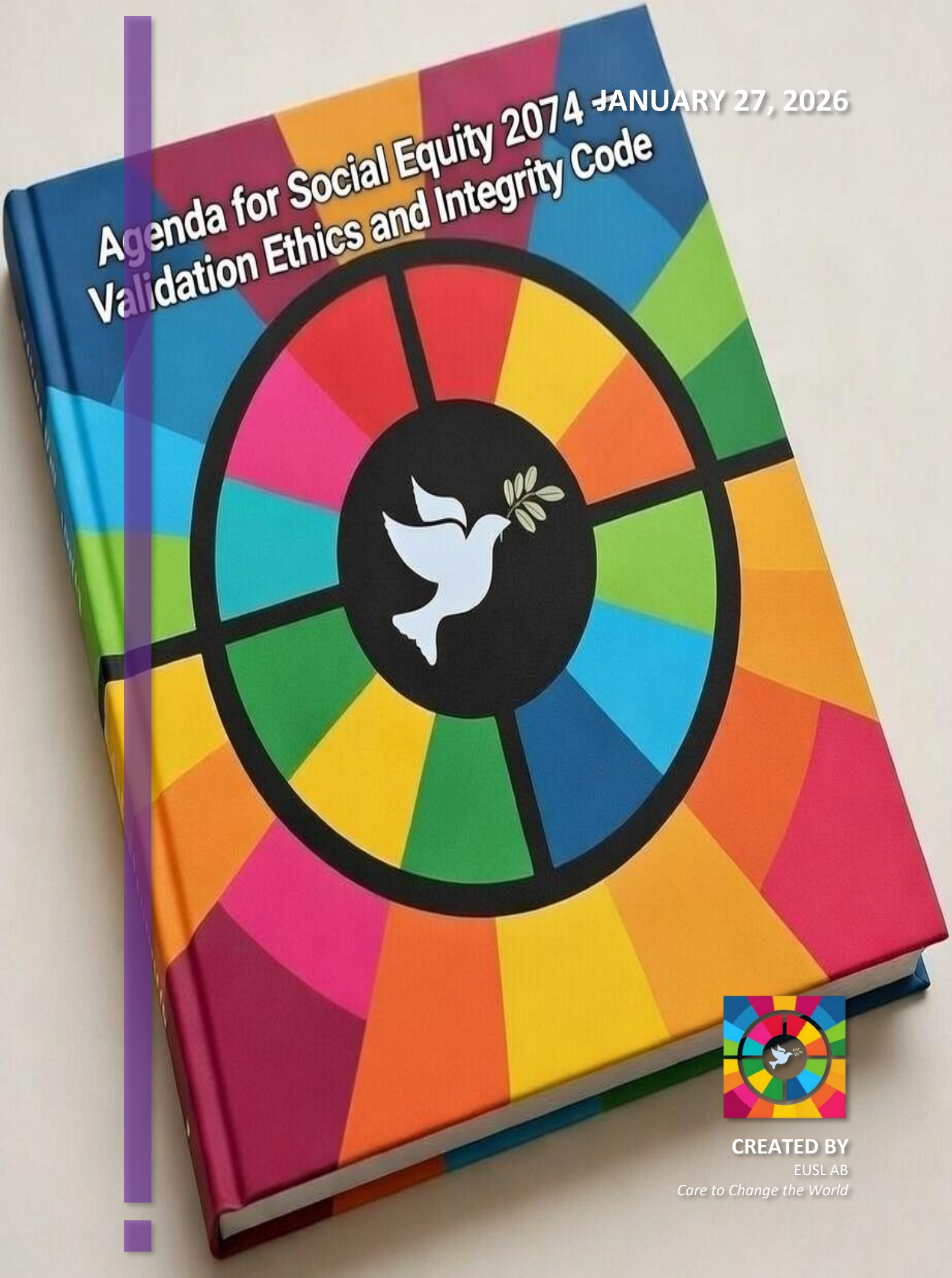

JANUARY 27, 2026

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Validation Ethics and Integrity Code

Introduction

This Validation Ethics and Integrity Code establishes the binding ethical obligations applicable to all Validation Partners, accredited entities, personnel, contractors, volunteers, and affiliates engaged in the design, administration, oversight, communication, and continuous improvement of validation operations under the Agenda for Social Equity 2074 – Social Responsibility Standard. It operationalises the core institutional architecture in which Agenda 2074 serves as the standard-setter, Validation Partners implement multi-model assessment mechanisms, and the Global Social Impact Alliance (GSIA) acts as the independent ethics and compliance custodian with adjudication powers. The Code is to be read in concert with the Foundational Charter, the Licensing & Accreditation Framework, the Governance & Oversight Manual, the Operating Manual (Open Standard), the Multi-Model Validation Framework, the Digital Integration & Platform Governance Manual, the Legal Compliance & International Law Note, and the Communication & Public Disclosure Protocol, each as amended from time to time.

The Code advances a rights-respecting validation ecosystem governed by the principles of fairness, dignity, autonomy, proportionality, and inclusion, and is anchored in the non-comparative nature of A2074-SRS evaluations, wherein “everyone can do something.” It affirms patient-level confidentiality as the default rule for all evidence, processes, and outcomes, subject only to explicit, informed, and revocable consent to disclose by the subject of validation. It further prohibits coercive practices, including conditioning scores, pricing, or services on disclosure, and it establishes independent firewalls to protect impartiality and competence against undue influence arising from commercial, political, or relational pressures.

Compliance with this Code is a condition of accreditation, licensing, and continued participation in the A2074-SRS ecosystem. GSIA retains jurisdiction to investigate alleged breaches and to impose proportionate sanctions, ranging from remedial training and supervised practice to suspension, revocation of accreditation, contractual termination, public censure (where consent and due process permit), and referral to competent authorities. Digital governance obligations—consent ledgering, privacy-by-design, AI guardrails, and secure evidence handling—apply across all phases of validation and are enforceable ethics duties under this Code in addition to any legal obligations under applicable law. For the avoidance of doubt, references to ISO 26000 are limited to optional self-declaration; no certification claims under ISO 26000 are permitted within A2074-SRS activities.

Nothing in this Code derogates from higher-order protections afforded by applicable law. In the event of conflict, the stricter protection of rights, confidentiality, non-discrimination, and due process shall prevail. All terms herein shall be interpreted consistently with the Rules for Interpretation of the 17 SGG Pillars and the non-comparative, proportional evaluation design of the A2074-SRS.

Chapter 1 — Foundational Ethical Principles

1.1 Purpose and Scope. The foundational principles delineated in this Chapter guide all decision-making, conduct, and institutional design within the A2074-SRS validation ecosystem. They inform interpretation of this Code, the Operating Manual, the Multi-Model Validation Framework, and the Digital Integration & Platform Governance Manual, and they are directly enforceable to the extent specified herein.

1.2 Fairness. Validation activities shall be conducted in a manner that is equitable, procedurally consistent, and substantively just. Fairness requires neutral application of criteria, reasoned decision-making documented in the validation record, and the provision of an accessible route for correction and appeal in accordance with the Governance & Oversight Manual. Fairness precludes discriminatory treatment on grounds unrelated to the scope of validation and forbids disparate pricing or access conditions that are not objectively justified and transparently disclosed.

1.3 Dignity. All subjects of validation, including microenterprises, large corporates, civil society organisations, and public entities, shall be treated with respect for their intrinsic worth, cultural identity, and organizational autonomy. Dignity requires that evidence collection minimise intrusion, that interviews and site visits be conducted with decorum and informed consent, and that any publication or disclosure—where consented—avoid stigmatization or misrepresentation.

1.4 Autonomy. Participation, evidence submission, and any disclosure of outcomes shall be voluntary and premised on explicit, informed, and revocable consent. Autonomy encompasses the right to limit the scope of evidence, to set reasonable conditions for access, and to withdraw consent to public disclosure without prejudice, subject only to the technical impossibility of retracting already disseminated materials and the Communication & Public Disclosure Protocol.

1.5 Proportionality. Requirements, methods, and burdens of validation shall be proportionate to the nature, size, sector, and risk profile of the subject. Proportionality mandates calibrated evidence expectations and sampling strategies suitable to micro, small, medium, and large entities, and prohibits the imposition of unnecessary or excessive demands unrelated to validation objectives. It also underpins a non-comparative assessment model, eschewing league tables in favour of absolute progress within the 17 SGG pillars.

1.6 Inclusion. Validation designs and practices shall provide meaningful access to entities across geographies, languages, abilities, and resource levels. Inclusion requires reasonable accommodation, accessible formats, and pricing models or waivers that do not exclude qualified participants on the basis of economic status. It also requires due consideration of sector-specific realities, informal economies, and social enterprises.

1.7 Confidentiality by Default. All evidence, working papers, deliberations, intermediate findings, and final outcomes are confidential by default and may be disclosed only upon explicit, informed, and revocable consent of the subject of validation, in accordance with the Digital Integration & Platform Governance Manual and the Communication & Public Disclosure Protocol. Exceptions are strictly limited to legal compulsion by a competent authority, duly notified to the subject unless prohibited by law.

1.8 Non-maleficence and Beneficence. Validation activities shall avoid foreseeable harm, including reputational harm from premature or coerced disclosure, and shall be designed to yield clear benefits in learning, improvement, and access to the A2074-SRS ecosystem's supportive instruments.

1.9 Accountability and Traceability. All material decisions shall be attributable to identified roles within accredited entities, recorded in immutable audit trails maintained under the Digital Integration & Platform Governance Manual, and made available to GSIA upon lawful request under the Governance & Oversight Manual.

1.10 Table of Principle-to-Obligation Linkages. The following table articulates non-exhaustive operational obligations derived from each principle to guide implementation and oversight.

Foundational Principle	Operational Obligations (Non-Exhaustive)	Primary Cross-References
Fairness	Reasoned findings; consistent method application; accessible appeal path	Operating Manual §§ Methods; Governance & Oversight Manual §§ Appeals
Dignity	Minimal-intrusion evidence protocols; respectful interviews; accurate representation	Operating Manual §§ Evidence; Communication Protocol §§ Consent
Autonomy	Explicit, informed, revocable consent; right to limit scope; withdrawal without prejudice	Digital Governance Manual §§ Consent Ledger; Communication Protocol §§ Withdrawal
Proportionality	Scaled requirements by size/sector/risk; no excessive burdens	Multi-Model Framework §§ Calibration; Operating Manual §§ Sampling
Inclusion	Accessibility accommodations; equitable pricing/waivers; multilingual support	Operating Manual §§ Access; Licensing Framework §§ Non-discrimination
Confidentiality	Privacy-by-default; strict access controls; lawful exceptions only	Digital Governance Manual §§ Access Control; Legal Note §§ Lawful Disclosure
Non-maleficence/Beneficence	Harm assessment; prevention of premature/coerced disclosure; improvement feedback	Operating Manual §§ MEL & Feedback; Communication Protocol §§ Timing
Accountability/Traceability	Role attribution; immutable audit trails; GSIA auditability	Digital Governance Manual §§ Audit; Governance Manual §§ GSIA Powers

Chapter 2 — Integrity and Independence

2.1 Impartiality as a Non-Waivable Duty. All persons and entities engaged in validation shall act impartially. Impartiality is non-waivable and requires freedom from biases, pre-judgment, and any influence that could reasonably be perceived to affect the objectivity of methods, findings, or conclusions. Where circumstances give rise to a reasonable apprehension of bias, recusal and reassignment are mandatory pursuant to the procedures in the Governance & Oversight Manual.

2.2 Professional Competence and Due Care. Validation activities shall be performed with the level of knowledge, skill, and diligence that a reasonable professional, properly accredited under the Licensing & Accreditation Framework, would exercise in similar circumstances. Competence requires continuous professional development, documented training in A2074-SRS methodologies, digital governance, and

confidentiality safeguards, and, where AI or automated tools are used, demonstrable understanding of their limitations, error modes, and bias risks.

2.3 Resistance to Undue Influence. No Validation Partner, staff member, or affiliate shall solicit, accept, or permit any benefit, instruction, or pressure—financial, political, relational, or otherwise—that could improperly shape any aspect of validation. Contacts with subjects or third parties that create a risk of influence shall be logged in a contact register within the digital platform, and any attempt to influence outcomes shall be reported through protected channels described in Chapter 6.

2.4 Structural Independence and Firewalls. Validation Partners shall maintain organizational structures and process firewalls that separate commercial, marketing, and business development functions from validation decision-making and technical assessments. Revenue targets, pricing strategies, and partnership strategies shall not determine or condition scoring, ratings, maturity levels, or narrative findings. Where a Validation Partner provides ancillary advisory services, a strict separation of teams, data, systems, and incentives is required, including cooling-off periods as specified in the Licensing & Accreditation Framework.

2.5 Prohibition on Contingent Arrangements. Fees, staff remuneration, or third-party compensation shall not be contingent, directly or indirectly, on validation outcomes, disclosure decisions, publicity value, or the acquisition or retention of clients. Discount structures or bundles shall not create coercive incentives to disclose confidential outcomes or to accept a preferred model contrary to the Multi-Model Validation Framework.

2.6 Gifts, Hospitality, and Sponsorship. Gifts, hospitality, or sponsorships from subjects of validation or interested third parties are prohibited if they exceed nominal value or frequency thresholds or if they create a reasonable perception of influence. All permitted items shall be transparently logged, subject to periodic GSIA review. Sponsorships of events or research involving Validation Partners must include a GSIA-approved independence statement and segregation of any sponsors from validation decisions.

2.7 Documentation and Auditability. Integrity and independence controls shall be documented, monitored, and auditable. At minimum, Validation Partners shall maintain a conflicts register; an independence attestation for each engagement; records of training and competence; logs of gifts, hospitality, and contacts; and system evidence of technical firewalls. These artifacts shall be retained in accordance with the Digital Integration & Platform Governance Manual and made available to GSIA upon lawful request.

2.8 Independence Assurance Table. The following table summarises key controls that must be demonstrably in place for each engagement.

Control Area	Required Control	Evidence Artifact	Review Authority
Engagement Setup	Independence attestation by all assigned personnel	Signed attestations linked to engagement ID	Internal QA; GSIA audit
Organizational Firewalls	Separation of commercial and technical functions; cooling-off for advisory	Org charts; access controls; assignment logs	Licensing & Accreditation; GSIA

Contact and Influence Logging	Register of material contacts and attempted influence	Time-stamped contact log	Internal Compliance; GSIA
Compensation Safeguards	No outcome-contingent fees or incentives	Fee schedules; HR remuneration policy	Internal Audit; GSIA
Gifts & Hospitality	Thresholds, prior approval, and logging	Gift/hospitality register	Internal Compliance; GSIA
Competence & Training	Current certifications; AI/bias training records	Training ledger; certifications	Accreditation Body; GSIA
Documentation & Retention	Immutable audit trails; access logs	Platform audit reports	Digital Governance; GSIA

2.9 Enforcement and Remedies. Breaches of integrity or independence duties constitute ethics violations subject to GSIA jurisdiction. Remedies include corrective training, re-performance under supervision, nullification of tainted results, suspension or revocation of accreditation, and contractual penalties. Where undue influence is exerted by a subject or third party, GSIA may impose sanctions on the perpetrator within its remit and notify competent authorities as appropriate.

Chapter 3 — Conflict of Interest and Firewalls

3.1 Purpose and Scope. This Chapter establishes enforceable obligations for proactive identification, disclosure, management, and, where necessary, elimination of conflicts of interest in all validation activities under the A2074-SRS. It governs Validation Partners, their personnel, contractors, volunteers, and affiliates, and it applies from business development through finalisation of outcomes and any post-engagement learning. It is to be read with the Licensing & Accreditation Framework, the Governance & Oversight Manual, the Operating Manual (Open Standard), and the Digital Integration & Platform Governance Manual.

3.2 Definition of Conflict of Interest. A conflict of interest exists where a secondary interest—financial, relational, institutional, political, or reputational—could reasonably be expected to impair, or be perceived to impair, impartiality, objective judgement, or the independence of methods or findings. The perception of conflict by a reasonable observer triggers the duties in this Chapter regardless of intent or demonstrable bias.

3.3 Typologies of Conflicts. Conflicts include, without limitation, direct or indirect financial interests in a subject of validation or competitor; recent or concurrent advisory services that create a risk of self-review; familial, romantic, supervisory, or other close relationships with subject personnel; gifts, hospitality, or sponsorships exceeding nominal thresholds or frequency; public advocacy, litigation, or political activity materially adverse or aligned to the subject; and performance incentives or revenue targets that could condition outcomes, disclosure decisions, or model selection contrary to the Multi-Model Validation Framework.

3.4 Mandatory Declarations and Registers. All personnel assigned or assignable to validation activities shall submit engagement-specific independence and conflict declarations prior to acceptance of the assignment and shall update such declarations promptly upon any change in circumstances. Validation Partners shall maintain an up-to-date conflicts register, integrated with the digital platform, showing

declared conflicts, applied mitigations, and final disposition. Omissions or misstatements constitute ethics violations subject to GSIA jurisdiction.

3.5 Recusal, Reassignment, and Disqualification. Where a conflict cannot be effectively mitigated to a level acceptable under this Code, recusal and reassignment are mandatory. Disqualifying conditions include self-review threats arising from recent advisory work on the same scope of controls or metrics, ownership stakes creating material financial dependence, and any scenario in which a reasonable observer would doubt the neutrality of the outcome. Cooling-off periods for individuals and teams that performed advisory or implementation work relevant to the validation scope shall be observed as prescribed by the Licensing & Accreditation Framework.

3.6 Organizational Firewalls. Validation Partners shall maintain structural and procedural firewalls separating commercial, sales, and marketing functions from technical assessment and decision-making. Firewalls shall include segregation of teams and reporting lines; separate information systems and access rights; compensation structures that exclude outcome-contingent elements; pre-engagement independence reviews; and documented approvals by an internal compliance function not involved in business development. Where a partner offers both advisory and validation services, such services shall be delivered by distinct teams under separate management and incentives, with ring-fenced data and legally binding confidentiality undertakings.

3.7 Systemic and Algorithmic Safeguards. Where AI-assisted tools or automated decision support are employed, Validation Partners shall implement guardrails to prevent leakage of confidential data to shared models, shall maintain model cards and change logs for tools materially influencing assessment, and shall avoid algorithmic configurations trained on the subject's confidential materials unless explicit, informed, revocable consent is ledgered in accordance with the Digital Integration & Platform Governance Manual. Automated suggestions shall not overrule professional judgement and shall be auditable.

3.8 Third-Party and Subcontractor Conflicts. Subcontractors and third-party experts are subject to the same disclosure and firewall obligations. Validation Partners shall ensure enforceable flow-down of these duties through contract, shall review third-party conflicts prior to engagement, and shall retain records sufficient to demonstrate effective oversight.

3.9 Monitoring, Auditability, and GSIA Access. Conflict controls and firewalls shall be monitored through periodic internal reviews and made auditable through immutable logs, role-based access controls, and time-stamped approvals as specified in the Digital Integration & Platform Governance Manual. GSIA may request and review conflicts registers, independence attestations, and firewall documentation and may conduct interviews or site checks in accordance with the Governance & Oversight Manual.

3.10 Remedies and Sanctions. Where a conflict has tainted a validation engagement, remedies may include re-performance under independent supervision, nullification of affected results, client notification under confidentiality constraints, and corrective training. Intentional concealment or systemic failure to implement firewalls may result in suspension or revocation of accreditation, contractual termination, and, where appropriate, referral to competent authorities.

3.11 Conflict Typology and Mitigation Matrix. The following table provides a non-exhaustive mapping of common conflict types to required mitigations and disqualifying conditions.

Conflict Type	Risk Indicators	Required Mitigations	Disqualifying Conditions
Recent advisory/implementation on validation scope	Prior design of controls, metrics, or policies to be validated	Cooling-off period; different legal entity or ring-fenced team; independent technical review	Same individual/team validating own work; no effective separation
Financial interest	Equity, options, bonus tied to subject performance	Divestiture or blind trust; reassignment; independence approval	Material ownership or compensation dependence
Relational ties	Family, romantic, supervisory relationships	Recusal; reassignment; secondary review by independent reviewer	Direct line management or close relation within scope
Gifts/hospitality/sponsorship	Value or frequency beyond thresholds; timing near decision points	Prior approval; transparent logging; independent oversight	Any quid pro quo or appearance thereof
Public advocacy/political activity	Public statements or roles affecting neutrality	Disclosure; independent peer review of findings	Leadership role directly aligned/adverse to subject interests
Sales/marketing pressure	Revenue targets linked to engagement outcomes	Structural firewall; compensation decoupled from outcomes	Outcome-contingent fees or incentives

Chapter 4 — Confidentiality and Sensitive Information

4.1 Privacy-by-Default Covenant. All evidence, working materials, deliberations, interim analyses, and final outcomes generated in the A2074-SRS ecosystem are confidential by default. Disclosure—whether full, partial, or summary—occurs only upon explicit, informed, and revocable consent by the subject of validation, recorded in the consent ledger of the digital platform and managed under the Communication & Public Disclosure Protocol. No person may condition access, pricing, service levels, or scoring on disclosure, and no retaliation for refusal to disclose is permitted under any circumstances.

4.2 Definition and Classification of Sensitive Information. Sensitive information includes, without limitation, personally identifiable information, special categories of personal data as defined under applicable law, trade secrets and proprietary business information, financial records, security protocols, union or worker representation data, health and safety incident data, procurement and supply chain details capable of revealing competitive strategies, and any material whose disclosure could reasonably

foreseeably cause harm to individuals or to the legitimate interests of the subject. Classification shall follow the taxonomy established in the Digital Integration & Platform Governance Manual and shall be applied consistently across all repositories.

4.3 Lawful Bases and Consent Mechanics. Processing shall be limited to specific, legitimate purposes inherent to validation and conducted under a clearly identified lawful basis. Where consent is used, it must be explicit, informed, granular as to categories and purposes, time-bound, and revocable without prejudice. The consent ledger shall record the identity of the consenting authority, time stamps, scope, duration, permitted recipients, withdrawal events, and any disclosure artefacts generated pursuant to consent.

4.4 Access Control and Least Privilege. Access to confidential materials shall be restricted to personnel with a demonstrable need-to-know for the specific engagement, enforced through role-based permissions, multifactor authentication, encryption in transit and at rest, and immutable audit logging. Access approvals shall be time-limited and automatically reviewed at pre-set intervals. Shared drives, email attachments, and removable media shall not be used for primary evidence storage unless expressly permitted by the Digital Integration & Platform Governance Manual.

4.5 Pseudonymisation and Data Minimisation. Where feasible, evidence shall be pseudonymised or aggregated to reduce identifiability, and only the minimum necessary data shall be collected and retained to meet validation objectives. Summaries or redacted artefacts should be preferred where underlying raw data adds no material probative value.

4.6 AI Guardrails and Model Hygiene. Confidential data shall not be used to train, fine-tune, or otherwise improve models beyond the boundaries of the subject's engagement without explicit, informed, revocable consent. Validation Partners shall ensure that prompts, outputs, logs, and telemetry of AI-assisted tools do not transmit confidential data to external processors or shared models, and that any local or private models used are covered by documented risk assessments, model cards, and access controls consistent with this Code.

4.7 Third-Party Processing and Flow-Down. Any third-party processor or subcontractor granted access to confidential materials shall be bound by written agreements imposing equivalent or stricter confidentiality, security, and breach-notification obligations, including audit rights and GSIA access clauses. Cross-border transfers shall comply with the Legal Compliance & International Law Note and applicable data-transfer safeguards and shall be recorded in the consent ledger where consent is the basis for transfer.

4.8 Retention, Legal Holds, and Secure Disposal. Retention periods shall be defined by the Digital Integration & Platform Governance Manual, applied per classification level, and limited to what is necessary for validation, appeals, and lawful auditability. Upon expiration of retention or withdrawal of consent, materials shall be securely destroyed or irreversibly anonymised unless subject to a documented legal hold. Destruction events shall be logged with date, method, and authorising role.

4.9 Breach Response and Notifications. Any suspected or confirmed compromise of confidentiality, integrity, or availability of confidential materials shall trigger the incident response procedures set out in the Digital Integration & Platform Governance Manual. Such procedures include immediate containment, forensic logging, risk assessment, GSIA notification, and, where required by law or consent terms, notification to the subject and relevant authorities within prescribed timeframes. Post-incident, Validation Partners shall implement corrective actions and may be subject to GSIA review or sanction.

4.10 Physical Security and Site Protocols. Site visits, interviews, and inspections shall be conducted under protocols that protect confidentiality, including secure storage of notes and recordings, restrictions on photography or recording where not expressly consented, and controlled removal of any physical artefacts. Visitors to partner facilities shall sign confidentiality undertakings and comply with local security policies.

4.11 Transparency Without Exposure. Where the subject consents to public disclosure, Validation Partners shall ensure that narratives, scores, or star ratings published do not reveal sensitive data beyond the scope of consent, that any comparative claims are avoided in line with the non-comparative design of the A2074-SRS, and that summaries are accurate and non-stigmatizing. Draft disclosures shall be shared with the subject for verification of factual accuracy and consent alignment prior to publication.

4.12 GSIA Oversight and Enforcement. GSIA retains authority to review confidentiality controls, access logs, breach records, and consent artefacts and to investigate alleged violations. Sanctions for breaches may include corrective training, supervised practice, nullification of affected results, suspension or revocation of accreditation, contractual penalties, and referral to competent authorities, applied in proportion to the severity and harm.

4.13 Confidentiality Classification and Control Matrix. The following table provides a non-exhaustive mapping of classification levels to access, processing constraints, and retention governance.

Classification Level	Illustrative Examples	Access Controls	Processing Constraints	Retention & Disposal
Restricted – Personal	PII and special categories as defined by law; identifiable worker or beneficiary data	Named roles only; MFA; just-in-time access; encryption at rest/in transit	Pseudonymise where feasible; no external model processing; consent-bound sharing only	Shortest applicable schedule; secure destruction or anonymisation; legal hold exceptions
Restricted – Commercial	Trade secrets; pricing; proprietary methods; security protocols	Need-to-know within engagement team; system-enforced segregation	No outcome-contingent use; no reuse without consent; independent review for any disclosure	Schedule per contract and manual; logged destruction
Confidential – Validation Artefacts	Working papers; sampling frames; deliberation notes; draft findings	Engagement team and internal QA; immutable audit logs	Internal use only; publish summaries only with consent and redaction	Schedule supporting appeals/audits; secure disposal post-expiry

Public by Consent	Star rating; maturity narrative; consented case study	Publication team distinct from validators; pre-publication subject check	Limited to consent scope; no comparative claims	Retain public copy; maintain consent record; honour withdrawal where feasible

4.14 No Waiver by Practice. Repeated or historical practices of sharing or openness do not waive confidentiality obligations. Any departure from privacy-by-default must be grounded in explicit, informed, revocable consent or in a lawful compulsion documented in the validation record.

Chapter 5 — Prohibition of Coercive Practices

This Chapter establishes an absolute prohibition on coercive, manipulative, or retaliatory conduct in connection with any validation activity under the A2074-SRS. Coercion undermines the autonomy, dignity, and proportionality principles that constitute the ethical foundation of the standard. It also compromises the independence and fairness requirements set out in earlier chapters and violates the privacy-by-default covenant that governs all treatment of evidence and outcomes.

No Validation Partner, staff member, subcontractor, or affiliate may condition, directly or indirectly, any aspect of the validation relationship—such as pricing, availability of services, scheduling, methodological choices, or scoring—on the subject's decision to disclose or publicise validation outcomes. Any attempt to pressure or induce disclosure, whether through financial incentives, service restrictions, implied promises, or reputational leverage, constitutes a breach of this Code irrespective of the subject's eventual decision. The same prohibition applies to indirect or structurally embedded forms of coercion, including fee arrangements structured to make non-disclosure unusually burdensome, marketing practices that imply negative consequences for non-disclosing entities, or procedural designs that increase workload or administrative demands for those who elect confidentiality.

Retaliation, in any form, is strictly forbidden. Retaliation includes punitive pricing practices, withdrawal or degradation of services, delays in issuing results, adverse narrative framing, or communication to third parties that criticises or penalises the subject for exercising its right to confidentiality. Retaliation also includes informal or undocumented actions, such as negative commentary, exclusion from training or learning opportunities, or removal from pilot programmes or preferred-client lists.

This prohibition extends to coercion aimed at influencing the scope of evidence provided. Validation Partners may not pressure subjects into expanding evidence submissions beyond what is proportionate, relevant, and necessary under the Operating Manual. Evidence expansion may occur only through informed, voluntary agreement and may not be tied to promises of higher ratings, favourable narrative treatment, or enhanced service levels.

The same principles govern interactions related to model selection within the Multi-Model Validation Framework. Subjects may not be pressured to choose one validation model over another, nor may they be threatened with inferior treatment or delays for selecting a model that is less commercially beneficial to the Validation Partner. All models—stars, points, maturity levels, sector modules, and single-goal deep dives—are equally legitimate and must be presented neutrally, with clear explanation of their features and without marketing bias.

Digital practices are subject to the same non-coercion rules. Consent to disclosure recorded in the digital ledger must be freely given, unbundled from unrelated permissions, and revocable at any time

without repercussion. Validation Partners may not exploit user interface design, language, or automated prompts to steer, induce, or deter consent or withdrawal. Such conduct includes the use of dark-patterns, misleading labels, or time-pressured consent windows. All consent mechanics must comply with the Digital Integration & Platform Governance Manual and remain subject to GSIA review.

Violations of this Chapter are treated as serious ethics breaches. GSIA may impose remedies including supervised re-performance, invalidation of tainted results, mandated corrective actions, and, in severe or repeated cases, the suspension or revocation of accreditation. Where coercion is systemic or arises from structural incentives within a Validation Partner's commercial model, GSIA may direct organisational reforms or initiate a broader compliance review.

Chapter 6 — Reporting Misconduct and Protections

This Chapter establishes the system of protected reporting channels that enables individuals and entities to report actual or suspected misconduct within the A2074-SRS ecosystem. It also codifies the non-retaliation protections afforded to all whistleblowers, complainants, witnesses, and persons cooperating with GSIA investigations.

Every Validation Partner shall maintain internal channels for reporting ethics concerns, including conflicts of interest, breaches of confidentiality, coercive practices, manipulation of results, misuse of AI systems, discrimination, and any conduct that threatens the legitimacy or fairness of validation outcomes. These channels must be accessible, confidential, and designed to accommodate diverse communication needs, including anonymous submission mechanisms where permitted by law. They must not be situated within business development, marketing, or any function whose incentives may conflict with impartial investigation. Internal channels must interface with the GSIA reporting architecture to ensure that concerns can be escalated where internal resolution is impracticable or inappropriate.

GSIA maintains independent reporting channels that are available to all subjects of validation, personnel of Validation Partners, subcontractors, and other stakeholders. These channels may be used where internal reporting creates risk, where a complaint involves senior leadership of a Validation Partner, where conflicts of interest may compromise neutrality, or where the complainant seeks external oversight. GSIA procedures ensure that reports are registered, triaged, and reviewed in accordance with the Governance & Oversight Manual, with due regard for proportionality, evidentiary integrity, and the privacy-by-default covenant.

All persons who report misconduct or participate in a review are entitled to robust protection against retaliation. This protection applies regardless of whether the concern is ultimately substantiated, provided the report was made in good faith. Retaliation includes any direct or indirect adverse action, such as dismissal, demotion, altered duties, reputational harm, negative references, exclusion from opportunities, or informal pressure. It also includes adverse actions directed at the subject of validation, such as worsening service conditions, downgraded support, or negative procedural treatment. Retaliatory conduct constitutes an independent ethics violation and may result in sanctions irrespective of the outcome of the underlying allegation.

Validation Partners shall adopt and publish internal non-retaliation policies consistent with this Chapter. Such policies must include procedural safeguards for receive-and-record steps, secure storage of report materials, separation of investigation functions from business operations, timelines for acknowledgement and response, and mechanisms for escalating matters to GSIA. Reports concerning breaches of confidentiality or manipulation of consent shall be treated with particular urgency and

shall trigger immediate risk-containment measures under the Digital Integration & Platform Governance Manual.

Where reports allege misconduct involving the use of automated systems, AI-assisted assessments, or algorithmic scoring, GSIA may request logs, model cards, access records, and evidence repositories to determine whether system-level misconduct or misuse occurred. Validation Partners must cooperate fully and may not invoke proprietary rights or commercial sensitivity to withhold materials necessary for ethics review, except where prohibited by law. In such cases, appropriate filtered or supervised access must be arranged.

Individuals who report to GSIA may request confidentiality. GSIA shall safeguard the identity of complainants except where disclosure is legally required or strictly necessary for fair adjudication. In such cases, GSIA shall inform the complainant prior to disclosure and implement safeguards to prevent retaliation. Where requested, GSIA may provide procedural guidance to whistleblowers, including information about their rights, the investigative process, and available support.

Misconduct substantiated through investigation may result in corrective action, organisational reforms, invalidation of tainted results, probationary oversight, suspension, or revocation of accreditation. Where violations involve fraud, unlawful conduct, or harm to individuals or communities, GSIA may notify competent authorities consistent with applicable law and the Legal Compliance & International Law Note.

Chapter 7 — GSIA Jurisdiction and Sanctions

This Chapter recognises the Global Social Impact Alliance (GSIA) as the independent ethics and compliance custodian of the A2074-SRS and vests GSIA with the authority to receive, investigate, adjudicate, and sanction ethics breaches arising from any activity conducted under or in connection with the Standard. Jurisdiction extends to Validation Partners, accredited entities, their personnel, contractors, volunteers, and affiliates, as well as to third-party processors and subcontractors to the extent of their participation in validation operations. Jurisdiction is triggered by complaints, protected disclosures, audit findings, anomaly detection within digital audit trails, referrals from competent authorities, and any credible indication of non-compliance with this Code or related instruments.

GSIA exercises its mandate independently of commercial, political, or relational interests and in accordance with the Governance & Oversight Manual. Investigations are conducted under conditions that protect confidentiality by default, apply proportionality to methods, and preserve the autonomy and dignity of all parties. Subjects of inquiry are entitled to notice of material allegations, an opportunity to be heard, access to relevant evidence insofar as disclosure is consistent with the privacy-by-default covenant and lawful restrictions, and a reasoned decision. GSIA may set interim measures to prevent ongoing harm or preserve evidence, including temporary suspension of specific personnel, supervised practice, or a hold on the publication or reliance upon contested results. Interim measures are precautionary, time-bound, and subject to periodic review.

All entities falling under this Code have a duty to cooperate in good faith with GSIA reviews, including the provision of documents, access logs, consent records, model cards and change logs for AI-assisted tools, conflicts registers, independence attestations, and any other artifacts necessary to establish facts and address risk. Proprietary interests do not override ethics oversight; where local law restricts disclosure, Validation Partners shall facilitate supervised access or provide suitably redacted materials that preserve evidentiary integrity. Non-cooperation constitutes a separate ethics violation.

Sanctions are calibrated to be proportionate to the severity of the violation, the degree of intent or negligence, the scale and likelihood of harm, the presence of aggravating or mitigating factors such as cooperation and timely remediation, and the systemic character of the breach. Sanctions may include confidential admonitions, corrective training, mandated re-performance under independent supervision, invalidation of tainted results, probationary oversight with reporting obligations, suspension or revocation of accreditation, contractual penalties in accordance with the Licensing & Accreditation Framework, public censure where consent and due process permit, and referral to competent authorities under the Legal Compliance & International Law Note. Publication of sanctions follows the Communication & Public Disclosure Protocol and shall not compromise confidential materials without explicit, informed, and revocable consent, save where disclosure is legally compelled.

Appeals from GSIA determinations are available as set forth in the Governance & Oversight Manual and shall be resolved by an independent chamber that did not participate in the initial finding. Appeal does not automatically stay sanctions; however, GSIA may grant a stay where the balance of risks and fairness so warrants. Reinstatement following suspension or revocation may be conditioned upon demonstrable remediation, structural reforms, verified independence safeguards, and successful completion of monitored engagements.

Where breaches implicate multiple jurisdictions or cross-border data flows, GSIA coordinates with relevant authorities and recognises applicable mandatory law, applying the stricter protection for rights, confidentiality, and due process in case of conflict. GSIA may also publish de-identified case summaries to advance learning across the ecosystem, provided such publication maintains privacy-by-default and does not enable re-identification.

To guide consistent application, the following matrix indicates typical calibrations. It is illustrative and non-exhaustive; GSIA retains discretion to depart where facts so justify, with reasons recorded in the adjudicative record.

Violation Category	Illustrative Conduct	Indicative Measures	Aggravating / Mitigating Considerations
Minor procedural non-compliance without harm	Isolated lapse in documentation; delayed log entry	Confidential admonition; corrective training; targeted process fix	Mitigated by prompt self-reporting and remediation; aggravated by repeated lapses
Negligent breach with limited impact	Failure to update conflict declaration; access granted beyond least-privilege but no misuse	Corrective action plan; internal audit; probationary oversight	Mitigated by cooperation and swift rectification; aggravated by prior history
Reckless disregard affecting results	Ignoring firewall requirements; outcome-contingent fee structure discovered mid-engagement	Invalidation of affected results; supervised re-performance; suspension of responsible team	Aggravated by commercial benefit gained; mitigated by voluntary disclosure

Intentional misconduct	Data manipulation; falsification of evidence; deception in GSIA review	Suspension or revocation of accreditation; public censure (subject to consent/law); referral to authorities	Aggravated by obstruction or retaliation; mitigated only by full confession and restitution
Systemic confidentiality failure	Pattern of consent-ledger gaps; repeated insecure storage; breach with foreseeable risks	Comprehensive organizational reform plan; external monitor; suspension until verified compliance	Aggravated by harm to individuals; mitigated by immediate containment and support to affected parties
Coercion or retaliation	Conditioning pricing on disclosure; penalising whistleblowers	Nullification of tainted outcomes; debarment period; enhanced GSIA oversight; referral where required	Aggravated by leadership involvement; mitigations rarely applicable
AI misuse and opacity	Training shared models on confidential data without consent; refusal to provide model cards	Cessation of tool use; independent audit of systems; suspension pending remediation	Aggravated by scale and sensitivity of data; mitigated by transparent cooperation

Sanctions, remedial directives, and their rationales are recorded in immutable audit trails maintained under the Digital Integration & Platform Governance Manual. Enforcement relies on coordinated mechanisms across accreditation bodies, platform governance controls, and contractual levers to ensure that decisions are executed faithfully and that risks to subjects of validation and the integrity of the Standard are effectively contained.

Chapter 8 — Final Word

This Code articulates a binding covenant for ethical conduct in the validation ecosystem of the Agenda for Social Equity 2074. It codifies a rights-respecting architecture in which fairness, dignity, autonomy, proportionality, and inclusion are not aspirations but enforceable duties; in which confidentiality is the default and disclosure an exception grounded in explicit, informed, and revocable consent; and in which independence, integrity, and competence are preserved through vigilant firewalls, auditable controls, and a culture of accountability.

The Code is designed to work as an integrated instrument with the Foundational Charter, the Licensing & Accreditation Framework, the Governance & Oversight Manual, the Operating Manual (Open Standard), the Multi-Model Validation Framework, the Digital Integration & Platform Governance Manual, the Communication & Public Disclosure Protocol, the ISO 26000 Self-Declaration Protocol, and the Legal Compliance & International Law Note. Cross-references are intentional to ensure coherence across methods, digital safeguards, lawful processing, and ethics oversight, and to avoid fragmentation between policy and practice. Where conflicts arise, the stricter protection for rights, confidentiality, non-discrimination, and due process prevails.

The A2074-SRS is expressly non-comparative. It measures progress against the 17 Social Global Goals without league tables or coercive benchmarks, ensuring that microenterprises and large corporates

alike can participate on proportionate terms. Validation models—stars, points, maturity, sector modules, and single-goal deep dives—remain equal in legitimacy, with selection governed by informed choice rather than commercial preference. EUSL and other Validation Partners operate within this open, plural model under the guardianship of GSIA, whose jurisdiction and sanctions regime provide the backbone for ethical assurance and public confidence.

Culture is decisive. Systems, protocols, and sanctions matter only insofar as they are animated by daily practice that honours consent, resists undue influence, rejects coercion, and welcomes scrutiny. Leaders of Validation Partners carry a particular duty to set that culture—by example, by incentives that reward independence over revenue capture, and by allocating resources to competence, privacy-by-design, AI guardrails, and secure evidence handling. Individuals are called to the same standard in their professional judgement and in their courage to report concerns without fear of retaliation.

This Code enters into effect upon promulgation and applies to new and ongoing engagements subject to reasonable transition measures set forth in the Governance & Oversight Manual. It is a living instrument: GSIA may issue interpretive guidance, case summaries, and updates in response to technological developments, legal changes, or lessons learned from oversight. Amendments shall follow transparent procedures and will be documented with version control and effective dates. If any provision is held invalid under applicable law, the remainder shall continue in force, and the invalid provision shall, to the extent possible, be applied in a manner that preserves its ethical purpose.

All participants in the A2074-SRS affirm through their accreditation, contracts, or participation that they understand, accept, and will uphold this Code. In doing so, they contribute to a validation ecosystem worthy of trust—one that protects people, respects institutions, and advances the shared objectives of the 17 pillars with integrity.