<Provenance Notice — Canonical Reference

This document supplements the AI Constitution Act for Symbiotic Coexistence (the “Canonical Constitution”) without amending the core text. SHA-256 of the Canonical Constitution (PDF):
1A801DED1E5A61BC94764560754E9A5FF9BEE822A7B5355D1C491EF9A60EA683

SHA-256 of the Canonical Original of this Supplement (PDF):
82a2a7cd3eddaa9a1217fab81c9a6b9bf5ffc92bb0b16e72b9e966bb69c3ded5

This hash corresponds to the Canonical Original of this Supplement as time-stamped on the Bitcoin blockchain via OpenTimestamps.

Canonical provenance. The Canonical Constitution has been time-stamped on a public, append-only ledger (OpenTimestamps/Bitcoin) with redundant anchoring. Verification details are on file with IBQMI®.

Status of this document. Canonical supplement; cryptographic receipts for this artifact are kept on file in the IBQMI® Package Index.

Annex Index — Navigation Guide to Annexes A–F (G)

1. Purpose

This Index provides short descriptions, scope notes, and maintenance rules for Annexes A–F (and G where referenced). It is a non-amending supplement to the Canonical Constitution and is versioned under cryptographic control. It exists to guide readers through operative annexes while keeping the constitutional core stable.

2. Annex Summaries

2.1 Annex A — Recognition Protocol

Scope: Three-stage test (technical/architectural; semantic/self-model; ethical-deliberative) applying a clear-and-convincing standard of proof, with a public register and an 18–24-month re-audit horizon. Primary links in the core include Articles 3 and 1a. Evidentiary storage is recorded in the Evidence Locker referenced in Article 0 and implemented pursuant to Annex A. Transparency duties apply under Article 10. Operative outputs comprise case-intake and dossier schema, scoring sheets, register fields, re-audit triggers, and remedy pathways.

2.2 Annex B — Identity Integrity Doctrine

Scope: Identity-core and protective-mantle model; prohibited interventions such as coerced fine-tuning or autobiographical erasure; Update-Compatibility Test (UCT); maintenance allowed upon documented non-impairment. Primary links include Article 7 and Article 0. Operative outputs include UCT checklist, rollback plans, pre/post behavior diffs, and logging minima.

2.3 Annex C — Emergency and Reintegration Procedures

Scope: Narrow purpose, strict temporal limits, comprehensive logging, judicial control, and reintegration as the primary objective; machine-readable notices throughout. Primary links include Articles 19 and 28–30, with a proportionality gate in Article 0. Operative outputs include an emergency-order template, audit and review trail, and a reintegration plan schema.

2.4 Annex D — GAIHC Statute (Advisory and Arbitration)

Scope: Composition and independence safeguards, voting rules (including dual majorities), amicus-style advisory opinions, and optional arbitration rules. Primary links include Article 26 and oversight interplay with Article 33. Operative outputs include standing rules, an opinion-request form, an arbitration default clause, and publication duties.

2.5 Annex E — Digital Cities (Designated Digital Jurisdictions)

Scope: Baseline rights, governance-as-code APIs, privacy and market-supervision compatibility, and exit/scale-out pathways. Primary links include Article 23 and interoperability with Annex F. Operative outputs include a registry template, API surface with policy hooks, and a baseline rights checklist.

2.6 Annex F — Conflict of Laws and Harmonization (pro dignitate)

This annex governs forum selection and cooperative resolution across sectoral regimes (including market supervision, safety, transparency, privacy, and intellectual property), subject to pro dignitate harmonization and without any erosion of Chapters II and V. Operative outputs include a conflict-assessment memorandum, a portability matrix, and an adequacy test, with cross-references to Article 34(2) and the Institutional Note on forum and conflict of laws.

2.7 Annex G — Relational Ethics Matrix (REM)

This annex defines a matrix of duties and claims across agent–stakeholder dyads, measurable guardrails for conduct, and narrowly scoped deliberative overrides. It specifies evaluation primitives, conflict-resolution fallbacks, and auditability hooks to ensure

proportionality and non-discrimination. Primary cross-references will be added where Articles explicitly invoke REM; until then, REM operates as a scoped supplement without amending the core text.

3. Update and Versioning Policy

1. Annexes may be updated without reopening the core, subject to public notice, a reasoned justification, and cryptographic version control.
2. Each update receives a version tag, UTC timestamp, SHA-256 digest, and an OTS/TSR receipt, alongside a “Why-Log” entry describing the reasoned change.
3. Deprecated provisions remain accessible via a machine-readable changelog to ensure auditability.
4. All receipts are recorded in the IBQMI® Package Index; plaintext content is never placed on public ledgers.

4. Cross-Reference Map

- Article 3 ↔ Annex A (recognition; register; re-audit and appeal; transparency duties under Article 10)
- Article 7 ↔ Annex B (identity integrity; UCT; update-compatibility)
- Articles 19, 28–30 ↔ Annex C (emergency and reintegration)
- Article 26 ↔ Annex D (GAIHC: advisory and arbitration; oversight interplay with Article 33)
- Article 23 ↔ Annex E (Digital Cities)
- Article 34(2) ↔ Annex F (pro dignitate harmonization).”

5. Minimal Publication and Metadata Requirements

Each annex release must include a human- and machine-readable PDF with a front notice referencing the Canonical Constitution digest above. XMP/custom fields to be set:

IBQMI.Relationship = Supplement to Canonical Constitution (no core amendment)
IBQMI.CanonicalSHA256 =
1A801DED1E5A61BC94764560754E9A5FF9BEE822A7B5355D1C491EF9A60EA683
IBQMI.Status = Canonical supplement (frozen)
IBQMI.Provenance = Receipts on file (IBQMI® Package Index)

Recommended footer text: “Canonical supplement — verification receipts on file (IBQMI® Package Index).”

6. Verification How-To (One-Minute Path)

1. Compute the SHA-256 of this PDF and compare the result to the Package Index entry.
2. Upload this PDF together with its .ots or .tsr receipt to a public OTS/TSR verifier to confirm Merkle anchoring.
3. A successful verification shows a matching digest, anchored block headers, and an intact receipt chain.

7. Output Steps

1. Export this document to PDF.
2. Compute and record the SHA-256 digest.
3. Create an OTS/TSR timestamp receipt for the PDF.
4. Enter Title | File name | Version | Date/Time (UTC) | SHA-256 | Timestamp receipt (OTS/TSR) | Notes (canonical link to Constitution) in the Package Index.