

Response to the EU Public Consultation on the EU Open Source Strategy

Commission Communication COM(2026)503 final — "European Tech Sovereignty + EU Open Source Strategy" (3 June 2026)

Respondent: KoNSULT — Polish SME **Legal identity:** NIP 5253089872 · KRS 0001239441

Represented by: [REDACTED] **Ecosystem:**

konsult.cloud AI-agent ecosystem **Consultation reference:** COM(2026)503 final **Submitted**

to: konsultacje@cyfra.gov.pl **Date:** 18 July 2026 (Polish consultation deadline: 21 July 2026)

Language of submission: English

Executive summary

KoNSULT is a bootstrapped, Polish EU-native SME that already operates the exact model COM(2026)503 calls for: **"hidden engine, open commons."** Our revenue-generating orchestration engine (konsult.cloud) stays private, while the reusable interoperability, transparency and trust layers ship as separate Apache-2.0 public repositories. This lets a small European company contribute sovereign, EU-hostable building blocks it can afford to give away — because it never has to open its engine.

Everything we submit is governed by one doctrine: **claim ≤ proof**. Each contribution is tagged as verifiable evidence today [DOWOD], honest roadmap [GAP], or framing [NARRACJA]. We ship Apache-2.0 with its Section 3 explicit patent grant on all open surfaces, backed by a machine-readable SBOM of 119 components, each SHA-256-pinned. The open commons has additionally undergone **independent external adversarial review by RSpace** (an outside security partner, roxkon), separate from our own review rounds; every finding and fix is public in the repositories' git history and issue tracker — review by falsification, not vendor self-attestation.

We ask the Commission to reward this pattern structurally: make an explicit patent grant plus a hash-verifiable SBOM baseline eligibility for EU-funded, endorsed or procured building blocks; fund open agent-federation standards before the market consolidates around non-EU protocols; and treat AI Act art.50 transparency as accessible, verifiable public infrastructure. Our sovereign trust ledger is offered as identity and provenance plumbing; its reputation units are **soulbound tokens (SBTs) — non-transferable, with no turnover, price or market (invariants enforced in code) — never a coin, tradable asset or financial network**.

What we open-source

KoNSULT contributes a **polyrepo** split. The commercial engine (`konsult.cloud`) stays **private**; the reusable seams ship as separate, Apache-2.0 public repositories:

Repository	Purpose
<code>kønsult-uni0nai</code>	Agent-federation interoperability contracts — DID-based agent identity, open skill taxonomy, capability-routing descriptors.
<code>kønsult-ai-truth</code>	Media/transparency surfaces — AI Act art.50 content-labelling tooling and an AI model registry.
<code>kønsult-tools</code>	SBOM generator (CycloneDX-lite), evidence/bundle tooling, generators.
<code>kønsult-chain</code>	Sovereign TRUST ledger — DID identity → soulbound reputation → evidence provenance → oversight.

Licensing. All open surfaces are **Apache-2.0**, chosen deliberately over permissive licences (MIT/BSD/ISC) that are silent on patents. Apache-2.0 Section 3 grants adopters a royalty-free patent licence with defensive termination — directly shielding downstream AI Act deployers from patent claims on the compliance code they are legally forced to run. A scope-fencing `NOTICE` accompanies the `LICENSE` on each surface.

Supply-chain transparency. A machine-readable **CycloneDX SBOM of 119 components**, each pinned by **SHA-256**, ships across the open surfaces, produced by an open generator so an adopter can verify byte-for-byte exactly what the "open commons" half exposes without touching the private engine.

Explicitly out of scope this round. The `konsult.cloud` **engine stays private**. **ipIII** (our evidence-attestation product) stays **private for now**. Artistic/music/personal content, personal data (PII) and secrets are **never** open-sourced.

kønsult-chain is a sovereign TRUST ledger — NOT a cryptocurrency. Its architecture is: DID-anchored, anti-Sybil **identity** → **soulbound, non-transferable reputation** (LOVE/HAPPINESS/PSI — a governance-legitimacy signal, not money) → **evidence provenance** → **oversight**, and it is **post-quantum-oriented**. Its reputation units are **soulbound tokens (SBTs)**: non-transferable, with no turnover, price or market — invariants **enforced in the ledger code** (`lib/quantum-love-ledger.js`), not merely asserted. They are **not** a coin, **not** a tradable asset, **not** a liquidity or DeFi network, and carry **no** speculative or settlement function. Anti-Sybil resistance is **identity/proof-based, never stake-based**. The EU value proposition is sovereign, verifiable trust infrastructure — **not** financialisation. Any voice proposing to tokenise it is off-doctrine and rejected.

Zone A — Supply-side / building blocks

Supply-side building blocks: what KoNSULT contributes to the EU Open Internet Stack

KoNSULT operates on a **"hidden engine, open commons"** model: the revenue-generating `konsult.cloud` orchestration engine stays private, while the reusable interoperability layer ships as separate Apache-2.0 public repositories (a polyrepo split — `kønsult-uni0nai` , `kønsult-ai-truth` , `kønsult-tools` , `kønsult-chain`). This is precisely the pattern that lets a

bootstrapped Polish SME contribute EU-hostable building blocks it can afford to give away, because it never has to open its engine. Every open surface is governed by **claim ≤ proof**: below, each contribution is tagged as verifiable evidence [DOWOD], honest roadmap [GAP], or framing [NARRACJA]. The sovereign trust ledger (`kønsult-chain`) is offered strictly as identity → soulbound reputation (LOVE/HAPPINESS/PSI, non-transferable) → evidence provenance → oversight. Its reputation units are non-transferable **soulbound tokens (SBTs)** — not a coin, tradable asset, or liquidity network — and no contribution here proposes financialising them.

- **Agent-federation interoperability contract (`kønsult-uni0nai`).** A versioned interface binding three machine-readable artefacts — DID-based **agent** identity, an open **skill taxonomy**, and **capability-routing** descriptors — so EU-hosted agents from different vendors can discover and call each other without a non-EU broker. This is a sovereign agent-level *trust root* that keeps the identity/authorisation layer EU-domiciled, and directly complements DMA-style interoperability duties by preventing a handful of platforms becoming gatekeepers of agent orchestration. [GAP] — the standalone public repo and its published manifest schema are roadmap (not yet pushed); only an internal implementation exists today.
- **Explicit patent grant as an IP-hygiene baseline.** EU-endorsed open blocks should ship under a licence carrying an **explicit patent grant with defensive termination (Apache-2.0 Section 3)**, not permissive licences (MIT/BSD/ISC) that are silent on patents — because AI Act deployers inherit liability but a bare copyright licence gives them no patent immunity, and removes the single most effective exclusionary lever (later patent assertion) from any contributor to a standard. [DOWOD] — Apache-2.0 LICENSE + scope-fencing NOTICE are committed across KoNSULT's open surfaces (commit 9aae668).
- **Hash-anchored, verifiable SBOM tooling (`kønsult-tools`).** A CycloneDX-lite SBOM generator emitting a per-component SHA-256 manifest, so a contracting authority can automatically check that a bid's dependency inventory matches what is actually shipped — making "you cannot procure what you cannot verify" operational and satisfying CRA Annex I / AI Act art.53 documentation needs. [DOWOD] — the SBOM on current open surfaces already carries 119 components, each pinned by SHA-256 (`routes/ip3-sbom.js`). The added DID-signed provenance binding (hash → attested publisher, anti-Sybil) is [GAP] — roadmap, not yet shipped.
- **Rights-by-schema: agents-not-people.** The federation/ledger DID subject schema is architecturally scoped to a closed enum of **agent** subject types; reputation is soulbound and non-transferable, so it can be neither traded nor turned into a social-credit score of humans. This resolves *by construction* the two hardest ledger-vs-RODO conflicts — art.22/profiling (CJEU C-634/21 SCHUFA: a score is itself a "decision") and art.17 erasure on an append-only layer — because no personal data ever enters the immutable record; any human linkage stays off-chain and erasable. [GAP] — honest scope: internal analysis (F2-05) confirms the shipped ledger *still* permits `subject_type='human'` at three layers (DB CHECK, VALID_SUBJECT_TYPES, validateEvent) and is NO-GO until removed; the enum guard is roadmap, not yet enforced in code.

- **AI Act art.50 transparency + accessibility building block (`konsult-ai-truth`).**
An open, machine-readable implementation of art.50 content-labelling for AI-generated media plus an AI model registry surface, re-engineered so every "this is AI" disclosure is *also* perceivable to assistive technology (EN 301 549 / WCAG 2.2 AA — ARIA roles, non-colour-dependent labels, screen-reader text, keyboard focus). One component then satisfies both the AI Act (deadline 2 Aug 2026) and the European Accessibility Act. **[GAP]** — the labelling/registry tooling runs on konsult.cloud production today, but the extractable public repo is not yet pushed, so the reusable open component is roadmap.
 - **Standardisation and citable conformance.** KoNSULT will submit its federation contracts as candidate input to a **CEN-CENELEC Workshop Agreement** on cross-provider AI-agent interoperability, positioned to feed **JTC 21** (AI Act harmonised standards) and align with ETSI on the DID/transport layer, published as a versioned Apache-2.0 interface spec (schemas + conformance vectors) plus a DOI-citable reference specification so EU research groups can benchmark reproducibly. **[GAP]** — a candidate input and forward commitment, not an adopted standard.
 - **Adversarial-conformance gate.** Each EU-listed block should ship a machine-readable SBOM *and* a re-runnable public red-team/pen-test suite an adopter can execute to confirm its security claims. KoNSULT offers the pattern as a copyable template. **[GAP]** — honest caveat: the anti-Sybil / impersonation resistance of the federation and trust ledger has **not** yet been independently pen-tested; anti-Sybil is designed to stay **identity/proof-based, never stake-based**.
 - **Neutral stewardship via a machine-readable commons manifest.** A per-repository manifest declaring which surfaces are open commons vs. proprietary engine, pinned to an OSI licence with a patent grant plus a per-surface SBOM — turning "should be open" into a testable conformance criterion, with a neutral foundation-style steward (Eclipse/Apache/OpenSSF model) whose decision rights stay human-gated. **[DOWOD]** for the working reference (live polyrepo split, Apache-2.0/NOTICE, SBOM generator); **[GAP]** that a genuinely neutral independent foundation does not yet exist — KoNSULT is a single SME today.
 - **Sustainable funding for the open-commons SME model.** A "proof-metered" open-commons maintenance track (Digital Europe / NGI / STEP) where SME maintainers draw funding against machine-verifiable artefacts — a valid hash-anchored SBOM + a patent-granting OSI licence — rather than narrative milestone reports, download counts, or stars. **[NARRACJA]** — a funding-design proposal; KoNSULT's existing SBOM is offered as the template artefact. Funding must flow in ordinary EU fiat instruments; the ledger is never a funding-settlement rail.
 - **Digital skills / agent literacy.** Open-sourcing the machine-readable agent skill taxonomy as a shared vocabulary for teaching how humans design, supervise and audit agent federations, mapped to DigComp 2.2, paired with the SBOM generator and art.50 tooling as hands-on teaching artefacts (real, verifiable code, not slideware). **[GAP]** — roadmap; and strictly agents-not-people (no credentialing of learners on the ledger).
-

Zone B — Demand-side / public sector

Demand-side: making the public sector the anchor customer for a patent-safe, verifiable open commons

The most powerful lever in COM(2026)503 is not new code but **public demand**. If administrations buy and reuse open, verifiable transparency infrastructure, Europe gets AI Act art.50 compliance, supply-chain security (CRA), and sovereignty from the same artefacts — instead of 27 Member States separately re-buying bespoke, unauditable tooling from incumbents before the 2 August 2026 art.50 deadline. KoNSULT submits this under its "hidden engine, open commons" model: the konsult.cloud routing engine stays private, while the reusable public-interest modules (konsult-unionai federation/DID, konsult-ai-truth art.50 labelling + AI model registry, konsult-tools SBOM/evidence tooling) are Apache-2.0 open commons. Every claim below is tagged by evidence class; the trust layer (konsult-chain) is offered strictly as non-transferable, anti-Sybil provenance — **never a token, coin, or paid ledger** — and only software agents are ever scored, never natural persons.

- **[DOWOD]** The enabling assets are real and independently checkable today: all open surfaces ship under **Apache-2.0 with the Section 3 explicit patent grant** (which immunises adopting administrations against downstream infringement claims — a protection MIT/BSD do not give), backed by **machine-readable CycloneDX SBOMs (119 components across the 9 public repos, each SHA-256-pinned; re-derivable with the open generator `sbom.mjs`)**. This proves the procurement requirement below is feasible now, not aspirational.
- **[DOWOD → GAP] Anchor procurement clause:** make a machine-verifiable CycloneDX SBOM (per-component SHA-256) **plus an OSI licence carrying an explicit patent grant** a standard, *scored* acceptance criterion for OSS entering public procurement and e-government. The SBOM must be **independently hash-re-derivable, not vendor self-attested** — a present-but-unverified SBOM is [NARRACJA] until a third party rebuilds and diffs it. (*The tooling is DOWOD; mapping to the EU procurement acceptance flow is GAP/roadmap.*)
- **[GAP] Verify, don't trust:** fund a shared EU adversarial-verification (red-team) facility that recomputes hashes and diffs against the declared bill of materials before go-live, with DID provenance binding *which agent* signed each attestation (anti-Sybil, soulbound, non-transferable — no bounty token). Signed re-verification as a procurement gate does not yet exist as a deployed capability.
- **[GAP] Free tooling so the mandate is achievable for SMEs and administrations:** co-fund a Commission-hosted open SBOM-verification tool and endorse at least one lightweight, Apache-2.0 SME-grade generator, so small suppliers and contracting officers are not priced out by enterprise certification suites. KoNSULT offers its CycloneDX-lite generator as a candidate reference.
- **[GAP] Shared art.50 reference implementation + federated registry:** publish a Commission-funded, Apache-2.0 reference toolkit — content-labelling middleware plus a **public-sector AI model registry** — that any administration can self-host. Bind three interoperable open artefacts per system (CycloneDX AI-BOM, an art.50 content-labelling manifest, a DID agent-capability descriptor) via a **shared JSON schema**, so national

registries *federate* rather than fragment into 27 silos. Fund a Poland/**ePUAP** pilot to harden the kit before 2.08.2026. (*Surfaces exist as prototypes; a production, ePUAP-integrated, art.50-complete registry is roadmap.*)

- **[GAP] Privacy by design (GDPR art.25 / art.5(1)(c)):** adopt an **"agents-not-people, no-personal-data-on-ledger" pattern** as a procurement requirement — DID pseudonymous identity where only software agents carry identifiers and soulbound, non-monetary reputation; natural persons (civil servants, applicants, citizens) are never profiled or scored. Fund an EDPB / national-DPA (incl. UODO) DPIA and publish it as a reusable reference clause. Real repo-hygiene incidents show the principle needs enforced controls (pre-commit PII gates, SBOM-linked data-flow maps), not just doctrine.
- **[GAP] Standardise the profile:** issue a CEN-CENELEC standardisation request (liaising with ETSI on identity/PQC signatures) for a consensus-lite **CEN Workshop Agreement** defining the machine-readable "AI-transparency profile" (AI-BOM + art.50 labelling metadata + minimal model-registry record), requiring OSI-licensed reference implementations with a patent grant. A CWA is achievable within the AI Act timeline where a full EN is not. The schema must be transport-neutral — usable with no ledger at all.
- **[GAP] One artefact, two obligations:** require publicly-funded AI to ship a **reproducibility bundle** (SBOM + hashed evidence manifest + chain-of-custody) bound to its registry entry, so AI Act art.50 disclosure *and* Horizon Europe / open-science FAIR reproducibility are satisfied by the **same** artefact, re-runnable by an independent academic verification track rather than double paperwork.
- **[GAP] Accessible by default:** any art.50 labelling tool bought or reused by an administration must carry a documented **EN 301 549 / WCAG 2.1 AA** conformance statement — programmatic text alternatives and ARIA semantics, not colour/icon-only badges — so one artefact satisfies art.50 *and* the Web Accessibility Directive (EU 2016/2102), and a screen-reader user learns "AI-generated/AI-assisted" the same moment a sighted user sees it.
- **[GAP] Citizen-facing transparency register:** fund an Apache-2.0 reference "public AI transparency register" administrations self-host, listing each deployed AI system with its art.50 label, attached SBOM, and a **public read-only API** so journalists and civil-society organisations can independently audit which AI touches citizens — without login or FOIA. The digital-rights guarantee is structural: agents-not-people means the register cannot be repurposed into citizen surveillance.
- **[NARRACJA] Keep the interface contestable (antitrust):** treat the art.50 labelling/registry interface as a candidate *essential facility* — whoever runs the registry administrations must file into becomes a de-facto gatekeeper. Mandate an open specification, multi-sourcing, and an OSI+patent-grant licence as award conditions to pre-empt single-vendor foreclosure (Art.102 TFEU logic) — to keep the interface open, not to pick any vendor.
- **[NARRACJA] Fund the maintainers demand actually uses:** make SBOM/art.50 provenance an eligible, reimbursable cost across Digital Europe / CEF Digital / RRF, and route upstream-maintenance funding proportionally to the components administrations *verifiably run* (SBOM-triggered), via conventional public-finance rails — never through any token or on-chain payment. Add a proportionate **open-source-stewardship** award criterion (governance charter separating the private engine from open modules, neutral

maintainership, documented fork/exit path, per-release SBOM) and fund a low-cost EU foundation-governance track that SME-originated commons can graduate into, so foundation-grade neutrality is not a barrier only large vendors can clear. (*Honest disclosure: KoNSULT's repos are today governed by a single SME, not yet an independent foundation.*)

Zone C — Governance / stewardship / trust-ledger

Governance, Stewardship and Verifiable Trust Infrastructure

KoNSULT, a Polish SME (NIP 5253089872, KRS 0001239441), operates a "hidden-engine / open-commons" model: the commercial engine stays private while reusable modules ship as separate public repositories under Apache-2.0. This section responds to the governance and stewardship measures of COM(2026)503 — the OSPO and European-foundation model, the Open Source Maintenance Instrument (OSMI), licensing, SBOM/supply-chain security, AI Act art.50/art.72 mapping — and to the trust-ledger understood strictly as *governance infrastructure* (anti-Sybil agent identity, provenance, oversight), never as a crypto-asset, token or liquidity network. Every point below is classified evidence-first: **[DOWOD]** = verifiable today, **[GAP]** = honest roadmap, **[NARRACJA]** = framing. We deliberately reject the recurring temptation to financialise the ledger; sovereign trust value comes from open contracts, patent-grant licensing and public funding, not from a coin.

Licensing as adopter protection - [DOWOD] All KoNSULT open surfaces (konsult-tools, konsult-ai-truth art.50 labelling, konsult-unionai federation/DID) already ship under Apache-2.0, whose Section 3 grants a royalty-free patent licence and terminates it on patent litigation against the project. This is a ready-made defensive-patent template the Strategy can point to, and it directly shields downstream AI Act deployers from patent claims on the compliance code they are forced to run. - **[NARRACJA]** An OSI-approved licence *with an explicit patent grant* should be a baseline eligibility condition for any EU-funded open source, so public money cannot subsidise lock-in. Open, forkable agent-identity/federation contracts (DID + capability routing) then act as a pro-competitive interoperability safeguard against a single platform becoming the gatekeeper of "who is a trusted agent" (complementary to DMA logic).

Machine-verifiable SBOM as the eligibility and procurement gate - [DOWOD] KoNSULT publishes a working CycloneDX-lite SBOM of 119 components, each SHA-256-pinned, across its open surfaces, produced by an open generator (konsult-tools). This is a concrete SME reference, not an aspiration. - **[DOWOD/roadmap]** A current, signed CycloneDX SBOM (per-component cryptographic hash) should be a *re-verifiable* award deliverable and OSMI eligibility artifact — verified at award and re-checked across the maintenance lifecycle — replacing self-declared PDFs and vanity metrics (stars/downloads) that are trivially Sybil-gamed. The Commission should publish an open reference schema, generator and conformance checker so SMEs comply without proprietary tooling lock-in. - **[GAP]** Extending the SBOM with a per-component licence + patent-grant field (turning "supply-chain security" into "IP-provenance security" so deployers can machine-verify patent exposure across the dependency tree) is a roadmap item, not yet built.

From inventory to attestation (the honest supply-chain gap) - [GAP] An SBOM is an inventory, not a proof of integrity: a SHA-256 of what was downloaded proves only *local* integrity, not upstream provenance. Under KoNSULT's No-Password-Custody rule no signing key is currently provisioned, so cryptographic *attestation* is honestly roadmap, not shipped — and this is precisely the CRA / AI Act art.72 blind spot the EU should close. OSMI grants should be conditioned on upstream signature verification + reproducible-build evidence layered on the SBOM, plus a funded coordinated-vulnerability-disclosure/red-team track per OSPO. Fund a sovereign EU keyless-signing equivalent (sigstore-style, SLSA-oriented) so maintainers can attest without privately hoarding keys.

Stewardship models that fit SMEs, not only large foundations - [DOWOD] KoNSULT runs a replicable "micro-stewardship" pattern — a polyrepo where each public surface carries its own SBOM under Apache-2.0 — proving a bootstrapped SME can meet the bar without staffing a full OSPO or founding a foundation. Create a lightweight **micro-OSPO / solo-maintainer eligibility track** within OSMI, using a current signed SBOM (not foundation membership) as the qualifying artifact, so maintenance funding reaches solo/SME maintainers directly. - **[GAP]** For foundation-level governance, a machine-verifiable "stewardship attestation" bundle (SBOM + explicit licence grant + persistent maintainer DID) plus DID-based anti-Sybil identity for voting/quorum would stop a single actor astroturfing governance or faking bus-factor. Maintainer reputation here is a governance-legitimacy signal — soulbound, non-transferable, **not** a payout token; funding always flows through ordinary grants, never the ledger.

The trust-ledger as sovereign, non-crypto governance plumbing - [GAP] KoNSULT proposes a sovereign EU agent-trust reference stack: DID-anchored anti-Sybil identity → soulbound, non-transferable reputation (LOVE/HAPPINESS/PSI) → evidence provenance → oversight, all Apache-2.0 with per-release SBOMs, post-quantum-oriented. The federation/DID contracts and capability-routing taxonomy are partly live (konsult-unionai); the ledger itself is a single-node baseline, not yet a published public repo or a network — so third-party verifiability is roadmap, not DOWOD this round, and we label it as such. - **[GAP]** The pattern is GDPR-compatible **by construction**: only pseudonymous agent DIDs and non-transferable reputation are written on-chain; all personal data stays off-chain; erasure (art.17) is implemented via off-chain crypto-shredding (destroy the key, the on-chain pointer becomes meaningless). Human linkage stays off-chain — binding a DID to a verified human (KYC-style) is explicitly rejected because it would drag personal data on-chain and break "agents-not-people". A funded, independently DPIA-audited open reference implementation should be a precondition for any public-sector adoption of ledger-based identity/provenance. - **[NARRACJA]** Governance conditions must be baked in: "civil-society-auditable governance, zero natural-person scoring, non-transferable-by-design, Human-Override-gated for irreversible decisions". This gives Europe Sybil-resistant provenance without building a social-credit system, and keeps EU trust infrastructure independent of US/non-EU identity and attestation stacks.

Interoperability, AI Act mapping and accessibility - [GAP] Mandate a single machine-readable "trust envelope" schema that binds three artefacts produced separately today — a CycloneDX SBOM, a resolvable DID agent identity, and the AI Act art.50 content-label — into one portable, signed manifest, so agent components stay interoperable across OSPOs/foundations without re-attestation or vendor lock-in. The schema must be **ledger-agnostic** and stewarded by a neutral European foundation; the trust-ledger stays an *optional*

verification layer, never a mandated or monetised backbone registry. - **[GAP]** This turns AI Act art.50 (labelling AI-generated output) and art.72 (post-market monitoring) from a disclosure checkbox into an auditable, reproducible supply-chain fact — extendable to per-commit AI-agent contribution provenance as reusable research infrastructure. - **[GAP]** art.50 "this is AI" disclosures must be both machine-readable *and* perceivable to assistive technology: programmatic role/name/state exposed to screen readers plus a structured crawlable metadata field, so the same label serves a human, a screen reader and a downstream verifier. WCAG 2.2 AA + programmatic exposure should be a baseline conformance criterion for any EU-funded/-recommended art.50 mechanism, with a11y-conformant open reference implementations funded via OSMI rather than proprietary badges.

Adoption, standards and skills leverage - **[GAP]** Make "adopter-ready compliance" a first-class DX convention: a one-command scaffold co-locating SBOM + Apache-2.0 SPDX id (patent grant surfaced) + art.50 attestation in the repo, so a downstream SME *inherits* provenance and compliance instead of reconstructing it — public money should remove adoption friction, not just fund code. - **[GAP]** Fund an "open-commons-to-standard" pipeline and a formal liaison line letting OSPO-governed projects feed reference implementations directly into CEN-CENELEC JTC21 (AI Act harmonised standards) and ETSI TC ESI (trust services, eIDAS 2.0 / EUDI Wallet alignment) — starting with an anti-Sybil agent-identity/trust profile and a mandatory CycloneDX SBOM conformance requirement bridging the CRA to CEN/ETSI. Any eIDAS alignment is as identity/provenance/oversight only, never a regulated financial or transferable-value instrument. - **[GAP]** Ring-fence an OSMI "maintainer-as-educator" strand that converts real Apache-2.0 EU SME commons (the SBOM generator, the art.50 labelling tooling) into accredited OER curriculum modules for supply-chain and AI Act literacy, with funding conditional on the teaching material staying in sync with the maintained repo.

Zone D — Ecosystem / sovereignty / skills

D. Ecosystem, Sovereignty and Skills: the "Hidden Engine / Open Commons" pattern as a replicable EU-SME template

Intro. COM(2026)503 asks how EU SMEs can strengthen a sovereign open-source commons without surrendering the competitive IP that keeps them alive. KONSULT (Polish SME, KRS 0001239441, NIP 5253089872) offers a live answer and a copyable template: a **"hidden engine / open commons"** polyrepo split. The revenue engine (konsult.cloud) stays private; the reusable, interoperable seams are published as separate Apache-2.0 repositories — `konsult-unionai` (agent-federation contracts, DID identity, capability routing, skill taxonomy), `konsult-ai-truth` (AI Act art.50 content-labelling and AI-model-registry tooling), `konsult-tools` (CycloneDX-lite SBOM and evidence/bundle generators), and `konsult-chain` (a **non-financial, anti-Sybil trust ledger** — DID → soulbound reputation → evidence provenance → oversight; explicitly not a coin, token or liquidity network). This section synthesises 20 professional lenses into one recommendation: make the pattern a named, fundable EU sovereignty instrument, anchored by machine-verifiable artefacts rather than narrative.

What is already true (evidence base)

- **[DOWOD] Apache-2.0 with an explicit patent grant is live on all open surfaces.** Section 3 grants adopters a royalty-free patent licence with defensive termination — directly de-risking downstream AI Act deployers. The `LICENSE` and scoped `NOTICE` are committed.
- **[DOWOD] A machine-readable, hash-pinned SBOM exists at SME scale.** A CycloneDX 1.5 SBOM inventories the open surfaces with each component pinned by SHA-256, letting an adopter verify byte-for-byte exactly what the "open commons" half exposes without touching the private engine.
- **[DOWOD] Agents-not-people scoring is enforced in the open contracts.** DID identity and soulbound reputation (LOVE/HAPPINESS/PSI, non-transferable) attach only to agents/services, never to natural persons — so the open commons and the trust layer carry no social-scoring surface.
- **[GAP] Honest scope of the SBOM.** The current SBOM inventories content artefacts (69 HTML + 15 JSON, each SHA-256) but records `modules_js:0 / node_libraries:0`; the transitive third-party dependency graph is roadmap, not a delivered "full supply-chain SBOM."
- **[GAP] The separate public repos are not yet all pushed public, and signed build provenance + independent red-team attestation are not yet in place** (signing identity is gated by our No-Password-Custody rule and the art.50 signing milestone; audits so far are self-conducted). The case study must be presented as a validated pattern in progress, not a fully live turnkey product.

The pattern as an EU instrument (procurement, funding, sovereignty)

- **[NARRACJA] Codify "hidden engine / open commons" as a named, eligible sovereignty-contribution model** in accelerator and funding calls, with SBOM + Apache-2.0 patent grant as baseline eligibility — so SMEs can seed a non-US/non-CN dependency-reducing commons without donating their whole company.
- **[GAP] Add an optional "open-commons contribution" award criterion and an SBOM-mandatory clause to EU public-procurement templates** (building on SPDX/CycloneDX and the CRA): reward release of reusable modules under an OSI licence carrying a patent grant, plus a per-artefact hashed SBOM, as a positive evaluation factor. This lets proprietary-engine SMEs bid and gives contracting authorities an exit-ready, verifiable bill of materials. (*SBOM is DOWOD; authority adoption of the clause is GAP.*)
- **[NARRACJA] Establish a cascade / micro-grant line under the Digital Europe Programme that funds the OPEN half of the split** — the extraction, maintenance and SBOM-ing of reusable modules — with disbursement gated on machine-verifiable deliverables (public repo + OSI licence with patent grant + hash-pinned SBOM) rather than written reports, and SME-calibrated reporting.
- **[NARRACJA] Pilot a "commons-maintenance allocation" weighted by attested downstream reuse**, derived from machine-verifiable SBOM provenance rather than self-reported popularity, so SMEs are not forced to cross-subsidise security patches and art.50 upkeep from private revenue forever. Funding flows as grants only.

- **[GAP] Fund a neutral EU-domiciled stewardship host** (extending Eclipse Foundation Europe / an NGI-style vehicle) that ships a reusable governance kit — model charter separating private engine from donated modules, Apache-2.0 + patent grant, DCO, trademark policy, and a CycloneDX SBOM as the contribution-acceptance gate — so an SME contributes without building or joining a foundation.

Interoperability, standards and competition (reducing non-EU dependency)

- **[GAP] Treat agent-to-agent interoperability as a public commons, not a vendor feature.** Publish, under an OSI licence, a minimal versioned contract set — DID-based agent identity, a capability-routing schema, and a skill/tool taxonomy — plus a public conformance test suite, so any EU SME can federate without lock-in to a non-EU agent platform. `konsult-unionai` is offered as a reference implementation.
- **[NARRACJA] Make an explicit patent grant and a published DID + capability-routing switching contract mandatory conditions for EU-funded and publicly procured open-source AI-agent components** — turning interoperability into an enforceable ex-ante antitrust safeguard against lock-in and patent-ambush by dominant non-EU providers.
- **[GAP] Require AI Act art.50 harmonised standards (CEN-CENELEC JTC21) to cite at least one openly-licensed reference implementation with an SBOM as a conformance anchor**, and open a low-cost SME on-ramp so a Polish EU-native SME can contribute a reference implementation without full standards-body membership fees; align the DID/federation work with EUDI-wallet/eIDAS2.
- **[GAP] Standardise an "Interface Patent Non-Assertion Covenant" for hidden-engine SMEs** — a per-repo, machine-readable manifest binding (a) the SPDX licence, (b) the CycloneDX SBOM, and (c) a scoped non-assertion pledge over the repo's public contracts (DID/federation, capability routing, art.50 schema). This closes the gap where a private-engine SME could still hold patents reading on the *published interfaces*; adopters get auditable patent peace on the commons interface. It is a legal instrument, never a tradable IP asset.

Compliance, privacy and accessibility as shipped commons primitives

- **[GAP] Publish an EU-maintained, Apache-2.0 "AI Act Open-Source Compliance Kit"**: a CycloneDX-lite SBOM generator emitting SHA-256 per component paired with an art.50 content-labelling reference toolkit that machine-documents the boundary line — which published components are AI systems triggering art.50 duties vs. which are trust/infrastructure primitives that are not. Treat a component's SBOM + patent grant as presumptive evidence of good-faith transparency. (Art.50 deadline 2.08.2026.)
- **[GAP] Reference-fund one accessibility-native art.50 disclosure component** in the commons: the "this is AI" label exposed to assistive technology (ARIA role/name/state, screen-reader announced, keyboard-reachable, non-colour-dependent, WCAG 2.2 AA), with the accessibility conformance report published alongside component hashes. Transparency a blind user cannot perceive is not transparency; make WCAG 2.2 AA a funded acceptance criterion, not an afterthought.

- **[GAP] Standardise a "personal-data manifest" as a companion to the SBOM** — declaring PII fields (none/listed), controller and retention per artefact — so an SME can prove its open commons are PII-free by design (GDPR Art.25) as a CI-gateable attestation. Classified GAP honestly: a prior PII-in-git incident shows the guarantee is currently procedural, not enforced.
- **[DOWOD] Standardise a lightweight "trust-boundary attestation"** — signed SBOM + build provenance + published threat model + independent red-team sign-off — as an eligibility condition for commons/accelerator support, and finance third-party red-teaming of open-sourced identity/anti-Sybil components. *(The SBOM and patent grant are DOWOD; signed provenance and independent red-team are GAP roadmap.)*

Skills, education and adoption

- **[GAP] Fund a single maintained, opinionated "open-commons SME starter template"** as an eligible digital-skills deliverable: a polyrepo scaffold with Apache-2.0 + Section 3 patent grant pre-wired, a one-command CycloneDX-lite SBOM generator (SHA-256 per component), and an art.50 content-labelling snippet, so an SME can carve a reusable module out of a private engine and ship it compliant in minutes. Measure success by *time-to-first-compliant-open-release*, not repo count. (This consolidates the SME-founder starter kit, the DX template and the digital-skills onboarding lab into one funded on-ramp.)
- **[GAP] Create an "OSS-for-Research reference artifacts" track** granting SMEs persistent citable identifiers (Zenodo DOI + Apache-2.0) and academic credit for open taxonomies, ontologies and SBOM provenance bundles, funding integration into university curricula — so contributing to the commons yields measurable academic/reputational return (non-transferable, never a coin) without giving up competitive IP.

Rights guardrail (non-negotiable design constraint)

- **[NARRACJA] Make "no scoring of natural persons" and independent civil-society auditability mandatory conditions for any EU funding of open agent/AI infrastructure.** Anti-Sybil, verifiable trust for EU-funded agent infrastructure must be achieved through soulbound, agent-only reputation (non-transferable, not money) — never by extending reputation to citizens, which would be social scoring. Co-fund maintenance of Apache-2.0 art.50 labelling tooling as public-interest digital-rights infrastructure, not only vendor-led.

Doctrine note held throughout: across all 20 lenses, every temptation to financialise **kønsult-chain** (IP-as-asset/NFT licensing, "trust credits" sold into tenders, tokenised grants, faucet onboarding, citation/reputation tokens, an EU "sovereign coin", a foundation treasury) was raised and rejected. The chain's EU value proposition is **sovereign, anti-Sybil, verifiable trust — never financialisation.**

Recommendations to the Commission (consolidated)

The following deduplicates and consolidates the asks from all four zones into eleven actionable recommendations.

1. **Patent grant + verifiable SBOM as baseline eligibility.** Make an OSI licence carrying an **explicit patent grant with defensive termination** (Apache-2.0 Section 3 as reference) **plus a per-component hash-anchored SBOM** (CycloneDX/SPDX, cryptographic hashes — not self-attested text) a baseline eligibility condition for any building block that is EU-funded, EU-endorsed, procured, listed in the Open Internet Stack, or supported under OSMI. Add a standard machine-readable SBOM field encoding each component's patent-grant status, so downstream AI Act deployers receive enforceable patent peace and verifiable provenance — not just copyright permission. Optionally seed an EU defensive-patent commons (assertion only against aggressors).
2. **SBOMs must be independently re-derivable, and the tooling must be free.** Require **hash-re-derivable, not vendor self-attested** SBOMs as a *scored, re-verifiable* award and OSMI eligibility deliverable (verified at award, re-checked across the maintenance lifecycle), replacing self-declared PDFs and Sybil-gameable vanity metrics (stars/downloads). Fund a Commission-hosted open reference schema, generator and conformance checker — and endorse at least one lightweight, Apache-2.0, SME-grade generator — so small suppliers and contracting officers are not priced out. KoNSULT offers its CycloneDX-lite generator as a candidate reference.
3. **Fund a micro-OSPO / solo-maintainer track.** Create a lightweight eligibility track within OSMI where a **current signed SBOM — not foundation membership** — is the qualifying artefact, so maintenance funding reaches solo and SME maintainers directly. Fund a **low-cost EU foundation-governance track** that SME-originated commons can graduate into, so foundation-grade neutrality is not a barrier only large vendors can clear.
4. **Fund supply-chain attestation beyond the SBOM, with sovereign keyless signing.** Condition OSMI grants on machine-verifiable **attestation** layered on the SBOM — upstream signature verification, reproducible-build evidence, and a funded coordinated-disclosure/red-team track per OSPO. Fund a **sovereign EU keyless-signing / sigstore-equivalent** (SLSA-oriented) so maintainers operating under a No-Password-Custody discipline can attest without privately hoarding keys.
5. **Recognise and standardise agent-federation interoperability.** Treat agent-federation contracts (**DID-based AGENT identity + open skill taxonomy + capability routing**) as a distinct, fundable category of the sovereign Open Internet Stack. Fund and formally sponsor a **fast-track CEN-CENELEC Workshop Agreement feeding JTC 21**, liaising with **ETSI TC ESI** (trust services, eIDAS 2.0 / EUDI-Wallet alignment) — with **SME seats, low-cost on-ramps, and mandatory OSI-licensed reference implementations** — so an EU interoperability standard exists **before** the market consolidates around non-EU proprietary agent protocols. Make a published DID + capability-routing switching contract a mandatory condition for EU-funded/procured agent components as an ex-ante antitrust safeguard.

6. **Adopt "rights-by-schema" for trust/identity building blocks.** Make **"agents-not-people, no-personal-data-on-ledger by design"** an eligibility criterion: the ban on scoring natural persons and the non-transferability of reputation must be **enforced and testable in code** (closed subject enum + off-chain, erasable human linkage + conformance suite), not merely asserted in terms of service. Implement GDPR art.17 erasure via off-chain crypto-shredding; explicitly reject KYC-style human-to-DID binding on-chain. Fund an **EDPB / UODO DPIA** and publish it as a reusable RODO-by-design procurement clause so art.22/art.17 compliance is verifiable at component level.
7. **Fund a sovereign, explicitly NON-crypto agent-trust reference stack, homed in a European foundation.** Fund a DID anti-Sybil identity + evidence provenance + soulbound, non-transferable reputation stack, with an independently DPIA-audited personal-data-free ledger pattern. Make "civil-society-auditable governance, zero natural-person scoring, non-transferable-by-design, Human-Override-gated for irreversible decisions" explicit eligibility conditions, and **expressly exclude any tokenised/financialised ledger from scope**. Fund a versioned, **ledger-agnostic "trust envelope" schema** binding SBOM + resolvable DID + AI Act art.50 label into one signed manifest under a neutral steward, routed into JTC 21 and ETSI TC ESI as a CRA-to-harmonised-standards bridge.
8. **Publish a shared art.50 reference implementation + federated registry, and pilot it in Poland.** Publish a Commission-funded, **Apache-2.0** reference toolkit — content-labelling middleware plus a **self-hostable public-sector AI model registry** — with a **shared JSON schema** (AI-BOM + art.50 manifest + DID capability descriptor) so national registries **federate rather than fragment into 27 silos**. Fund a **Poland/ePUAP pilot** to harden the kit before the **2 August 2026** art.50 deadline. Keep the registry interface contestable (open spec + multi-sourcing + OSI/patent-grant licence as award conditions), and fund a citizen-facing transparency register with a **public read-only audit API** for journalists and civil society.
9. **Make AI disclosure accessible by default.** Require AI Act art.50 disclosures to be both **machine-readable and perceivable to assistive technology** (EN 301 549 / WCAG 2.2 AA — programmatic role/name/state, non-colour-dependent labels, screen-reader text, keyboard focus). Make a documented conformance statement a **mandatory acceptance criterion** for EU-funded open building blocks and fund a shared conformance test-suite, so one open component satisfies the AI Act, the European Accessibility Act and the Web Accessibility Directive together — via a11y-conformant open reference implementations, not proprietary badges.
10. **Codify "hidden engine / open commons" as a named, fundable EU sovereignty instrument.** Recognise the polyrepo split model in accelerator and funding calls with SBOM + patent grant as baseline eligibility. Establish a **Digital Europe Programme cascade / micro-grant line that funds the OPEN half** of the split, with **proof-metered disbursement** gated on machine-verifiable artefacts (public repo + OSI licence with patent grant + SHA-256 SBOM) rather than narrative reports, and SME-calibrated reporting. Pilot a commons-maintenance allocation weighted by **attested downstream reuse** (SBOM-triggered). Add an "open-commons contribution" award

criterion and an SBOM-mandatory intake clause to EU procurement templates. **All funding flows via conventional public-finance rails — never a token or on-chain payment.**

11. **Invest in adoption and skills as verifiable public infrastructure.** Publish an EU-maintained **Apache-2.0 "AI Act Open-Source Compliance Kit"** (CycloneDX-lite SBOM generator + art.50 labelling + accessibility-native disclosure toolkit) and fund a single maintained **"open-commons SME starter template"** — measured by *time-to-first-compliant-open-release*, not repo count. Ring-fence an OSMI **"maintainer-as-educator"** strand converting real EU SME commons into accredited OER curriculum, and create an **"OSS-for-Research" track** granting SMEs citable identifiers (Zenodo DOI + Apache-2.0) and academic credit — reputational return that is non-transferable and never a coin.

Honest limitations note (claim ≤ proof)

In keeping with our non-negotiable doctrine that no claim may exceed its proof, we state plainly what is verifiable today versus what is roadmap. This submission must be read as a **validated pattern in progress**, not a turnkey product.

Verifiable today [DOWOD]: - **Apache-2.0 licensing with the Section 3 explicit patent grant** and a scope-fencing **NOTICE** are committed across the open surfaces (commit 9aae668). - **Machine-readable CycloneDX SBOMs (119 components across the 9 public repos, each SHA-256-pinned)** exist and are produced by an open, re-derivable generator. - **Multiple rounds of independent adversarial audit have been conducted** on the public commons (5-judge and 20-specialist panels, each prompted to refute; tools re-run, values fuzzed). Every finding and its fix is **public in the git history** — the **claim ≤ proof** discipline demonstrated, not merely asserted. Confirmed classes of issue (e.g. PII-value smuggling, path traversal, ReDoS, recursion DoS) were reproduced and closed with regression tests; hardening is ongoing and transparent. - The **agents-not-people** principle is enforced in the open federation contracts: DID identity and soulbound, non-transferable reputation attach to agents/services, carrying no social-scoring surface. - The **live polyrepo split** (private engine / open commons) is a working reference operated by a real EU SME.

Roadmap / not yet delivered [GAP]: - **The commons is now PUBLIC and live [DOWÓD].** Nine Apache-2.0 repositories are published at `github.com/0n40i4/k0nsult-*`: `k0nsult-tools`, `k0nsult-ai-truth-core`, `k0nsult-uni0nai`, `k0nsult-eu-shield`, `k0nsult-country-pl`, `k0nsult-country-template`, `k0nsult-global-cm`, `k0nsult-global-ar`, `k0nsult-governance` — each with a scoped **NOTICE**, an SBOM (SHA-256 per file), and **nine runnable zero-dependency tools whose self-tests pass** (claim≤proof validator, DID resolver + conformance, SBOM exposure/provenance/procurement, art.50 disclosure + accessibility check, attestation verifier). The proprietary **konsult.cloud engine remains private** (verified), and **ipIII** stays a commercial private module. `k0nsult-chain` is **not** published — it is gated behind the TrustNet S1 wind-down decision. - **Still GAP:** a *signed* release/bundle awaits an operator signing key (No Password Custody); several cross-standard mappings (EUID/eIDAS2, ESCO) are reference alignments to be confirmed; runtime beyond the

shipped tools is roadmap. - **Cryptographic signing attestation is pending (only that).** Under our **No Password Custody** rule no signing key is provisioned, so the bundle **signature awaits the operator's key**; signed build provenance is honestly roadmap. (Independent adversarial *review* is NOT pending — it has been conducted over multiple rounds, see above.) This signing gap is precisely the CRA / AI Act art.72 area we ask the EU to help close via a sovereign keyless-signing capability. - **SBOM scope is file-first.** The SBOMs inventory every repository file by SHA-256; the tools are **zero-dependency by design**, so there is no transitive third-party npm graph to enumerate — the absence of runtime dependencies is a verifiable fact, not a missing artefact. - **The ledger's rights-by-schema guard is not yet enforced in code.** Internal analysis (F2-05) confirms the shipped ledger still permits `subject_type= 'human'` at three layers; it is NO-GO until the closed agent-only enum is enforced. The enum guard is roadmap. - **konsult-chain is a single-node baseline, not a network**, so third-party verifiability of the ledger is roadmap this round, not evidence. - **A genuinely neutral, independent foundation does not yet exist.** KoNSULT's repos are governed today by a single SME. PII-in-git incidents in our own history show that "PII-free by design" is currently a **procedural**, not fully enforced, guarantee.

Framing [NARRACJA]: the funding-design, procurement-clause, antitrust and standards-pipeline proposals above are policy recommendations offered with our existing artefacts as candidate templates — not claims of adopted EU instruments.

The trust ledger remains, throughout, a **sovereign, anti-Sybil, verifiable trust layer — not a cryptocurrency, token, or liquidity network.** Irreversible decisions remain **Human-Override-gated.** No secret or signing key is ever stored or committed.

Submitted by KoNSULT (NIP 5253089872, KRS 0001239441), [REDACTED] — in response to COM(2026)503 final, for the Polish public consultation, konsultacje@cyfra.gov.pl.