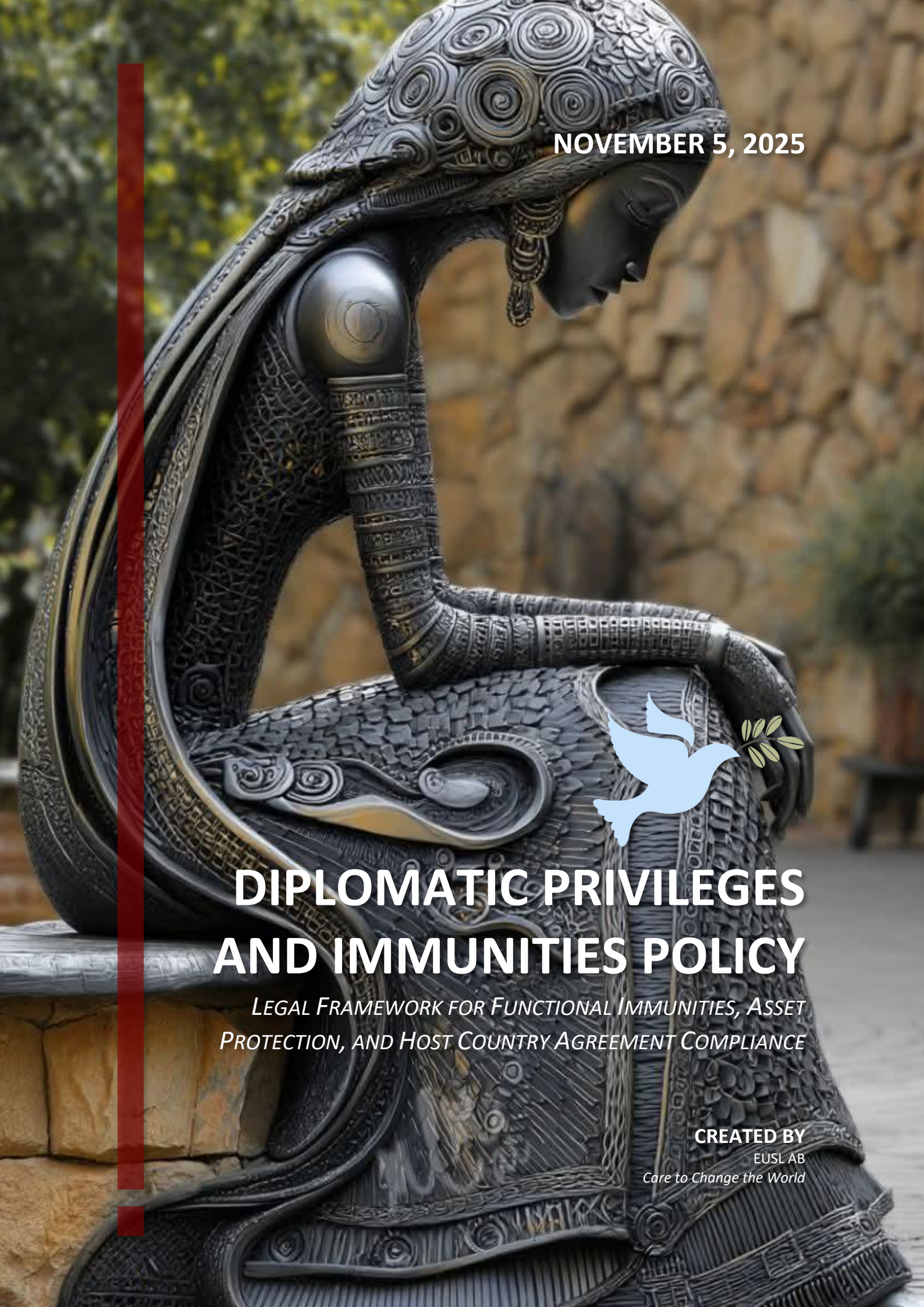

NOVEMBER 5, 2025

DIPLOMATIC PRIVILEGES AND IMMUNITIES POLICY

Legal Framework for Functional Immunities, Asset Protection, and Host Country Agreement Compliance

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Diplomatic Privileges and Immunities Policy

Preamble and Applicability. This Policy is promulgated under the GSIA Charter and shall be read consistently with Documents 00–15 and the established order of prevalence: mandatory national public law; the GSIA Charter; this Policy; and downstream instruments and annexes. The constitutional allocation of functions remains binding. The GSIA SCE holds mandate and oversight; GSIA Holding AB maintains canonical standards, clause libraries, evidence taxonomies, and model Host Country Agreement (HCA) provisions without operational entanglement; GSIA AB conducts programme operations under Service Level Agreements (SLAs); DESA-class entities (e.g., SUDESA, CODESA, and regional/national DESA units) act as recipient-operators under Flowhub custody; and, where required for bankability and continuity, Hosted Ownership may be used within ring-fenced perimeters subject to non-attachment, negative pledge, discrete ledgers and bank accounts, and an unconditional reversion covenant to the Member upon readiness. Publication remains a control, with lawful redaction and time-limited deferrals by reasoned resolution entered in the deferral register. Controller/processor roles are explicit; DPIAs are conducted for high-risk processing; identity and access management (IAM) enforces least-privilege with multi-factor authentication; logs are immutable and time-synchronised; encryption is mandatory in transit and at rest. Domestication follows the gated progression—shadowing → dual-key → lead-role → system handover → legal localisation → readiness certification—and is verified under Document 09.

Chapter 1 — Functional Immunities for Staff

1.1 Purpose and Constitutional Position. Functional immunities are limited legal protections necessary to safeguard the independent performance of GSIA's public-interest mandate. They are strictly functional, applying only to acts performed in an official capacity under the Charter, SLAs, Implementation Agreements (IAs), and HCAs or equivalent instruments. Functional immunities are not personal privileges and shall not be construed to shield private conduct, negligence beyond official acts, or criminal wrongdoing.

1.2 Scope of Persons and Roles. Functional immunities may be accorded, by reasoned HCA or equivalent instrument, to: (i) designated officials of the GSIA SCE acting in oversight; (ii) GSIA AB staff and secondees performing programme duties under SLA; (iii) DESA officials and staff while executing programme tasks as recipient-operators; and (iv) Agenda 74 Agency personnel when mandated as initial performers. Eligibility lists are maintained, published with lawful redaction, and updated through reasoned resolutions.

1.3 Substantive Protections. In accordance with the HCA or equivalent, the following limited protections may be granted for official acts: (i) immunity from legal process (civil and administrative) for statements made and acts done in the course of official duties; (ii) inviolability of official papers and documents, including digital records, subject to lawful inspection protocols agreed in advance; (iii) tax and customs facilitation for official consignments and equipment necessary to discharge programme functions; and (iv) expeditious visa, entry, and work-authorization processing for designated officials and experts on mission. These protections are tailored by jurisdiction and shall not exceed what is strictly required.

1.4 Waiver and Accountability. Functional immunity is granted to protect the mandate, not the individual. The **GSIA SCE** (or a delegated officer designated in the **HCA) may waive immunity in any case where immunity would impede the course of justice and can be waived without prejudice to the mandate. Waiver decisions are reasoned, recorded, and published with lawful** redaction. Nothing herein derogates obligations to cooperate with competent national authorities, subject to agreed protocols preserving confidentiality of sensitive programme information.

1.5 Limits and Exclusions. Functional immunities do not apply to: (i) traffic and safety offences unrelated to programme duties; (ii) private contracts or personal liabilities; (iii) criminal acts outside official capacity; (iv) defamation or harassment outside official communications; or (v) conduct violating GSIA's Compliance, Audit, and Ethics Code (Document 11). Alleged abuse triggers investigations under Document 11, with possible sanctions, dismissal, referral to authorities, and publication consistent with lawful redaction.

1.6 Interaction with Publication and Data-Protection. Requests from authorities for access to official documents are handled under the publication doctrine and data-protection rules (Document 12). Where compelled disclosure is sought, GSIA invokes the agreed HCA process for in-camera or controlled access, preserving chain-of-custody and confidentiality while enabling law-enforcement objectives. DPIAs are mandatory for any disclosure involving personal data; access is logged immutably.

1.7 Verification and Evidence Handling. The existence and scope of functional immunities are documented in the HCA or equivalent and published with lawful redaction. Eligibility registers, appointment letters, and mission orders are maintained as evidence of official capacity. Any assertion of immunity must be supported by these records, which are reviewable by the SCE Assurance and Standards Committee and, where relevant, by independent validators under Document 09.

1.8 Domestication and Sunset. Functional immunities are time-bound and sunset upon completion of official duties or termination of the programme in the host jurisdiction, subject to survivals for acts performed during the period of duty. As domestication gates advance and public custodianship expands, reliance on functional immunities shall decrease and be replaced by standard administrative protections available under national law.

1.9 Hosted Ownership Alignment. When Hosted Ownership is used, functional immunities granted to operational staff do not modify ring-fencing, negative pledge, non-attachment, or the reversion covenant. Immunities shall not be invoked to frustrate external validation, audit, or step-in rights; controlled access protocols guarantee evidence availability without compromising the mandate.

Chapter 2 — Asset Protection

2.1 Purpose and Constitutional Position. Asset protection ensures the inviolability, lawful custody, and exclusive programme use of GSIA-administered assets, physical and digital, to prevent diversion, encumbrance, or seizure inconsistent with the Charter, HCAs, Implementation Agreements, Leasing Schedules, and Flowhub doctrine. Asset protection provisions preserve fiduciary integrity, verifiability, and continuity during domestication and after handover through survivals expressly stipulated.

2.2 Asset Taxonomy. For purposes of this Policy, assets include: (i) financial assets (cash in discrete bank accounts, hedging receivables/payables, escrow balances); (ii) tangible assets (equipment, vehicles, labs, ICT infrastructure); (iii) intangible assets (software licences, cryptographic keys, data models, templates, IP curated by GSIA Holding AB); and (iv) digital-evidence assets (logs, MEL repositories,

forensics images, integrity artefacts). Asset registers are maintained at portfolio and project levels, published in summary with lawful redaction, and reconciled to discrete general and sub-ledgers.

2.3 Ring-Fencing and Non-Attachment. All programme assets are held within ring-fenced perimeters featuring: (i) discrete bank accounts and ledgers; (ii) negative pledge clauses prohibiting collateralisation or guarantees for unrelated liabilities; (iii) non-attachment preventing seizure or set-off by third parties outside the perimeter; and (iv) cash waterfalls prioritising essential obligations, liquidity buffers, safeguards, MEL, and capped Flowhub commission (≤5% absent Charter-conforming amendment), with no private distribution. These protections are codified in HCAs, IAs, and Leasing Schedules.

2.4 Inviolability of Premises and Repositories. Premises, depots, and secure data repositories used for official purposes are inviolable to the extent agreed in the HCA and limited to programme needs. Entry by authorities requires prior notification and a joint access protocol with GSIA representatives present, except in acute emergencies defined by law. For digital repositories, access is mediated through IAM approvals, break-glass procedures, and immutable logging; decryption keys are managed under dual-control and split-knowledge with key-ceremony records.

2.5 Custody, Control, and Title. Custody is exercised under Flowhub or an approved equivalent. Title may vest in DESA, a Hosted Ownership SPV, or the Member, as specified in the governing instrument. Where title is hosted, a reversion covenant requires transfer to the Member or designated public custodian upon readiness certification or cure of ineligibility, with survival of audit rights, record retention, warranties, and liabilities as stipulated. Title lists, serials, and location metadata are maintained and reconciled; transfers are notarised and published with lawful redaction.

2.6 Protections against Seizure and Expropriation. HCAs and IAs include non-seizure and non-expropriation clauses for programme assets, subject to mandatory national public law. Where lawful compulsion exists, GSIA invokes compensation and continuity provisions, including escrow release for essential services, and may apply step-in to preserve health, safety, and fiduciary integrity. Disputes follow the Legal Instruments Compendium without prejudicing emergency protective measures.

2.7 Data and IP Stewardship. Canonical data models, taxonomies, process libraries, and methods curated by GSIA Holding AB remain under its stewardship and may be licensed to DESA and Members on non-exclusive, royalty-free terms for public-interest use, subject to publication doctrine and data-protection safeguards. Software licences and configurations are inventoried; transfer or assignment upon handover is executed per vendor terms, with security baselines preserved.

2.8 Evidence Preservation and Forensics. Digital-evidence assets (logs, imaging sets, MEL evidence) are preserved under chain-of-custody, cryptographic hashing, and notarised inventories. Any access, duplication, or transfer requires reasoned approval, least-privilege IAM, and immutable logging. Destruction follows approved retention schedules and is documented with verifiable erasure certificates; exceptions (e.g., litigation hold) are reasoned and time-limited.

2.9 Insurance, Risk Transfer, and Continuity. Asset protection is complemented by insurance placements and hedging per Document 10 (Insurance and Hedging). Policies name the proper custodian (DESA/Hosted SPV/Member) and reflect ring-fencing, loss-payee, and claims-cooperation clauses. Business interruption parameters align with continuity targets (RTO/RPO). Claims proceeds are credited only to ring-fenced accounts and utilised for restoration; no private distribution is permitted.

2.10 Publication and Transparency. Asset protection clauses in HCAs, IAs, Leasing Schedules, and custody annexes are **published** with lawful redaction. Asset registers, reconciliations, transfer notices, and insurance placements are disclosed in summary. Deferrals for security or procurement integrity are reasoned, time-limited, and entered in the deferral register with sunset review.

2.11 Data-Protection and Sovereignty. Asset metadata that constitutes personal data is processed under controller/processor allocations and DPAs. Localisation and sovereignty requirements are respected via in-country hosting or escrow; cross-border transfers use lawful mechanisms with supplementary measures. IAM, encryption, and immutable logging apply at all times.

2.12 Domestication and Exit. Asset protection provisions are embedded from inception and tighten during shadowing and dual-key. At lead-role, custodial operations shift to DESA/Member teams under GSIA oversight. System handover includes asset registers, title instruments, key ceremonies, and documentation escrow. Legal localisation ensures registries and filings comply with national law without diluting ring-fencing. Readiness certification requires unqualified or acceptably qualified assurance over asset custody, records, and survivals. Exit and wind-down follow Document 10; inventories and reconciliations are validated and published.

2.13 Records, Survivals, and Assurance. Asset registers, title instruments, custody logs, access approvals, claims files, transfers, reconciliations, and publication records are archived per the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, IP stewardship, negative pledge and non-attachment until closure, and publication registers. Independent validators may be commissioned under Document 09 to opine on asset-protection conformity.

Chapter 3 — Comparative Treatments

3.1 Purpose and Method. This Chapter provides a comparative policy treatment to ensure that any immunities and asset-protection measures extended to GSIA through HCAs or equivalent instruments remain functional, proportionate, and consistent with the Charter across jurisdictions. It establishes a reference framework against which proposed privileges are benchmarked, ensuring that they (i) protect the public-interest mandate; (ii) preserve fiduciary controls, publication doctrine, and data-protection duties; and (iii) do not create personal privileges or derogations that would impair accountability.

3.2 Functional Immunity vs. Personal Privilege. Immunities contemplated herein are strictly functional: they attach to acts performed in an official capacity and never to the person as such. Personal tax exemptions, private customs allowances, or general inviolability not necessary for official duties are out of scope. Where host practice proposes broader privileges, GSIA shall accept only those elements demonstrably necessary to secure independence of official functions, documented by reasoned justification and sunset provisions.

3.3 Institutional Spread and Role-Based Differentiation. Comparative treatment differentiates between:
a) **GSIA SCE officials** performing oversight and standard-setting;
b) **GSIA AB** operational staff and secondees under SLAs;
c) **DESA** officials and staff acting as recipient-operators; and
d) **Agenda 74 Agency** personnel serving as initial performers.
Protections may vary by role and exposure. For example, inviolability of official papers and digital repositories may be broader for inspection and audit teams carrying evidentiary archives, while

visa/work-authorisation facilitation may be central for deployment teams. In all cases, protections remain bounded by official necessity and are subject to waiver (Chapter 1).

3.4 Interface with National Regimes. National legal regimes differ materially in their approach to immunities, asset security, data sovereignty, and public procurement. Comparative treatment requires that HCA provisions be localised to the host's public-law architecture without diluting core safeguards. Where national law provides equivalent or superior protections (e.g., statutory inviolability of audit records or protected disclosure regimes), GSIA relies on those instruments and narrows bespoke clauses accordingly. Where national regimes are silent or weaker, HCAs supply the necessary protections narrowly tailored to official needs.

3.5 Enforcement, Remedies, and Waiver Practice. Comparative analysis standardises waiver decision-making: immunities are waived where they would impede the course of justice and can be waived without undermining the mandate. Remedies for seizure or interference with programme assets prioritise continuity and restitution rather than damages; interim measures (escrow releases, step-in, controlled access to repositories) are pre-authorised in HCAs. All waivers, refusals, and remedies are reasoned, recorded, and published with lawful redaction.

3.6 Evidence and Publication Harmonisation. To avoid jurisdictional disparities in transparency, comparative treatment stipulates a minimum publication floor: (i) HCA operative clauses on functional immunities, asset protection, inspection protocols, and dispute logic; (ii) eligibility registers for protected officials; (iii) access protocols and redaction/deferral resolutions; and (iv) transfer notices and reconciliations at handover. Local requirements for secrecy (e.g., ongoing investigations) are respected through time-limited deferrals, with sunset review and re-publication upon expiry.

3.7 Data-Protection and Sovereignty Alignment. Immunity and asset-protection clauses cannot derogate from lawful controller/processor allocations, DPIAs, localisation mandates, or subject-rights where applicable. Where sovereignty rules restrict export of personal data or evidentiary artefacts, comparative treatment requires on-shore escrow and cryptographic integrity artefacts (hashes, timestamps) to preserve verifiability for external validation and audit. IAM, encryption, and immutable logging apply uniformly.

3.8 Domestication and Sunset Trajectory. As domestication proceeds from shadowing to readiness certification, reliance on HCA immunities and asset-inviolability is reduced and ultimately sunset. Comparative treatment embeds graduated sunset clauses tied to domestication gates and readiness certification. Post-handover survivals (audit rights, records, warranties, liabilities as stipulated) remain in force for defined periods; broader immunities lapse.

3.9 Hosted Ownership Consistency. Where Hosted Ownership is invoked, comparative treatment ensures that asset inviolability, non-attachment, negative pledge, discrete ledgers and bank accounts, and reversion mechanics are uniform across jurisdictions. Immunity clauses shall never be used to frustrate audit, external validation, or lawful step-in; controlled access protocols guarantee evidence availability.

3.10 Dispute Forums and Coordination. Comparative treatment aligns dispute logic across HCAs with the Legal Instruments Compendium to avoid fragmentation. Where multiple forums exist (administrative review, domestic courts, arbitral panels), coordination orders prevent duplication and preserve essential programme continuity measures. Appeals and publication follow established doctrine.

Chapter 4 — Host Country Agreement Provisions

4.1 Purpose and Structure. This Chapter sets out the model provisions for Host Country Agreements (HCAs) or equivalent instruments, to be localised to national law while preserving GSIA's constitutional safeguards, publication doctrine, data-protection obligations, domestication gates, and Hosted Ownership controls. Each clause is drafted to be severable, so that any invalidity does not defeat the remaining protections.

4.2 Parties, Purpose, and Definitions. The HCA identifies the Host (competent ministry/authority), the GSIA SCE, and—where applicable—GSIA AB, DESA recipient-operators, and Agenda 74 Agency as mandated initial performers. It states purpose: enabling GSIA-mandated programmes in the public interest with functional immunities for official acts and asset-protection for programme assets under Flowhub custody (or approved equivalent). Definitions track the Charter and the Legal Instruments Compendium (e.g., Flowhub, ring-fencing, non-attachment, negative pledge, domestication gates, controller/processor, DPIA).

4.3 Recognition of Legal Personality and Capacity. The Host recognises the GSIA SCE's legal personality and its capacity to contract, acquire/hold property for programme purposes, and participate in legal proceedings, subject to functional immunities for official acts. DESA entities are recognised as recipient-operators eligible to hold title and operate ring-fenced accounts and ledgers; Agenda 74 Agency is recognised as initial performer where mandated.

4.4 Functional Immunities for Official Acts. The Host accords functional immunities necessary for the independent performance of official duties: (i) immunity from legal process for statements made and acts done in official capacity; (ii) inviolability of official papers and documents, including digital repositories, subject to agreed access protocols; (iii) customs and tax facilitation for official consignments; and (iv) visa, entry, and work-authorisation facilitation for designated personnel. Waiver rests with the GSIA SCE (or delegated officer) and is exercised where justice would be impeded and waiver does not prejudice the mandate. Abuse or misconduct outside official acts is excluded.

4.5 Asset Protection and Custody. Programme assets are held within ring-fenced perimeters with discrete bank accounts and ledgers, negative pledge, non-attachment, escrow and cash waterfalls, and four-eyes approvals with segregation of duties and calibrated countersignature thresholds. The HCA prohibits seizure, set-off, or encumbrance of programme assets except as permitted by mandatory national public law, and then only through controlled access protocols that preserve continuity and chain-of-custody.

4.6 Title, Hosted Ownership, and Reversion. Where Hosted Ownership is required, the HCA recognises the approved SPV (e.g., EUSL) as lawful title holder within a ring-fenced perimeter, subject to a binding reversion covenant transferring legal and beneficial title to the Member or designated public custodian upon readiness certification or cure of ineligibility. Title lists and inventories are maintained; transfers are notarised and published with lawful redaction; survivals—audit rights, record retention, warranties, liabilities—are expressly preserved.

4.7 Data Protection, Sovereignty, and Digital Trust. The HCA affirms controller/processor allocations for public-interest processing; requires DPAs for processing by GSIA AB and vendors; mandates DPIAs for high-risk processing; and recognises localisation requirements. Evidence escrow and cryptographic integrity artefacts are used where export is restricted. IAM, immutable logs, and encryption are baseline obligations. Requests by authorities for access to official data follow in-camera or controlled access procedures, preserving confidentiality and chain-of-custody.

4.8 Publication and Transparency. The HCA codifies publication as a control: operative clauses (immunities, asset protection, custody, data protection, domestication, dispute logic) are published with lawful redaction; deferrals are reasoned, time-limited, and recorded with sunset review. Funding, commission, grant/pool registers, procurement awards, rectification dockets, and handover notices are disclosed per the Financial Transparency regime (Document 13).

4.9 Procurement Integrity and ESG Safeguards. The HCA incorporates by reference GSIA's ESG and fiduciary standards and confirms compatibility with host procurement law, applying the more stringent rule where conflict arises unless mandatory national public law prevails. Sanctionable practices (fraud, corruption, collusion, coercion, obstruction) trigger protective measures (payment holds, scope reduction, step-in) and referral to Investigations under the Compliance, Audit, and Ethics Code (Document 11).

4.10 Domestication, Handover, and Sunset. The HCA embeds the domestication gates and ties any exceptional protections to **sunset** on readiness certification, subject to survivals. It prescribes system handover protocols (key ceremonies, documentation escrow, configuration baselines), legal localisation requirements (registrations, mandates, signatory matrices), and readiness certification criteria (unqualified or acceptably qualified assurance over core controls, data governance, fiduciary propriety).

4.11 Continuity, Insurance, and Risk Transfer. The HCA recognises continuity obligations and permits **insurance** and hedging per Document 10. Loss-payee, claims cooperation, and restoration clauses are standard; proceeds are credited only to ring-fenced accounts with no private distribution. Continuity targets (RTO/RPO) are referenced; emergency access protocols are defined to preserve essential services.

4.12 Dispute Resolution and Coordination. Disputes follow the Legal Instruments Compendium. The HCA identifies the competent forum(s), coordination mechanisms to avoid duplication, emergency relief to preserve continuity, and publication of outcomes with lawful redaction. Appeals to GSIA's Appeals Board concerning administrative decisions (transparency, sanctions) are preserved without fettering judicial or arbitral remedies.

4.13 Term, Amendment, and Termination. The HCA states term, amendment procedures by reasoned, published resolution, and termination grounds. Exit and wind-down follow Document 10, preserving survivals, publication of inventories and reconciliations, and orderly transfer or reversion of assets.

4.14 Records, Survivals, and Assurance. The HCA mandates archival of registers, eligibility lists, access protocols, title instruments, reconciliations, and related records for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, IP stewardship, negative pledge and non-attachment until closure, and publication registers. Independent validation (Document 09) may be commissioned to opine on HCA compliance.