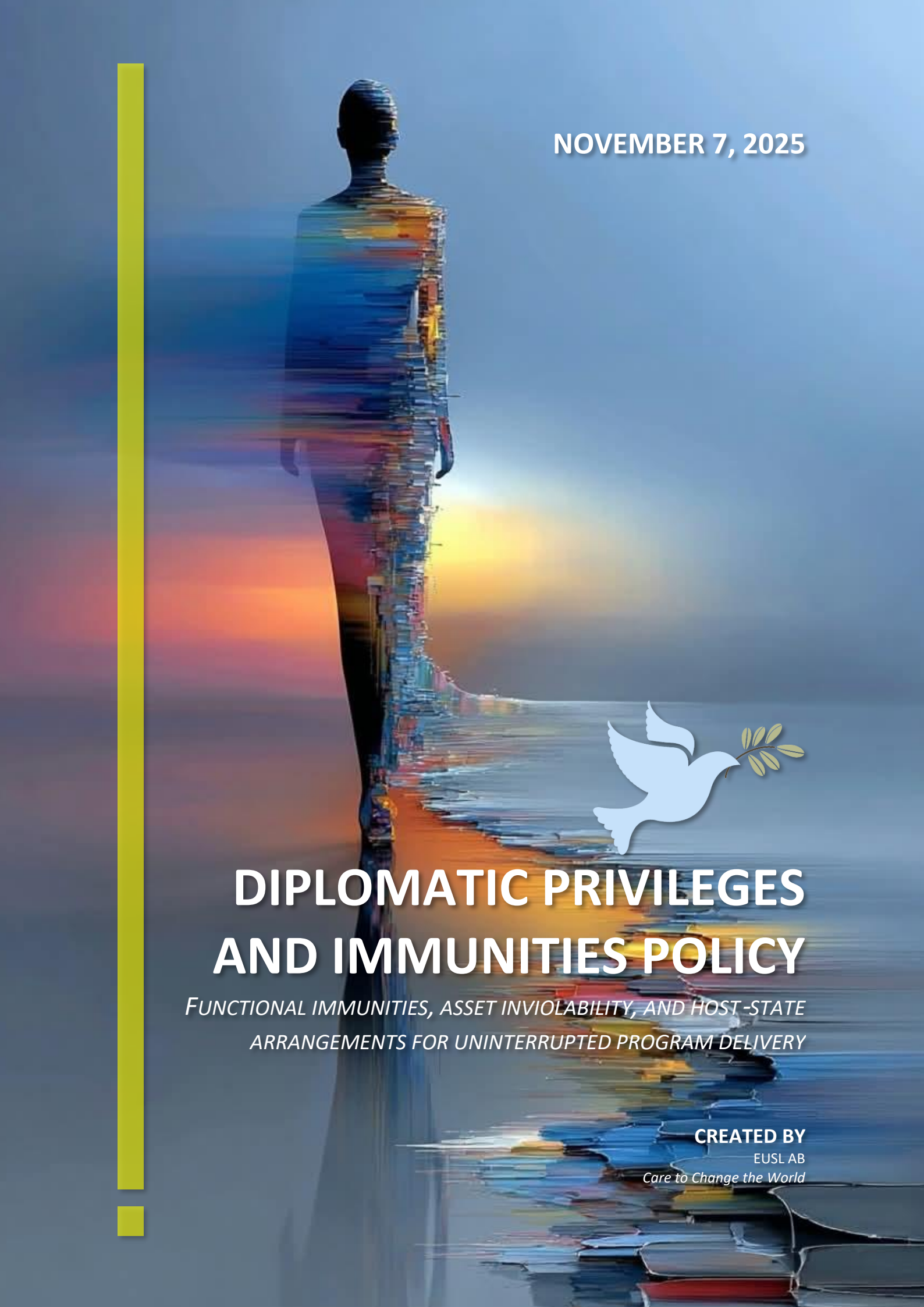

NOVEMBER 7, 2025

DIPLOMATIC PRIVILEGES AND IMMUNITIES POLICY

FUNCTIONAL IMMUNITIES, ASSET INVIOLABILITY, AND HOST-STATE ARRANGEMENTS FOR UNINTERRUPTED PROGRAM DELIVERY

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Diplomatic Privileges and Immunities Policy

Preamble

This Policy establishes the legal framework governing functional immunities, asset protection, and related privileges for Creativa Center ecosystem entities operating under Host Country Agreements. It ensures compliance with international law principles, including the Vienna Convention on Diplomatic Relations (1961), while adapting these norms to the sui generis nature of public–private partnerships under Agenda 2074. The Policy safeguards operational independence, fiduciary integrity, and continuity of essential services, while maintaining transparency and accountability obligations under Documents 06 (ESG Safeguards), 11 (Compliance Code), and 13 (Funding Framework). It is harmonized with global standards on governance, anti-corruption, and data protection, including UNGPs, OECD Guidelines (2023), ISO 37001, ISO 37301, and GDPR.

Chapter 1 – Functional Immunities for Staff

Functional immunities shall be narrowly tailored to the official acts necessary for implementing Creativa programs under Host Country Agreements, ensuring operational independence without derogating from accountability. Immunities are functional, not personal, and apply exclusively to acts performed in the discharge of official duties under instruments such as the Program Cooperation Agreement (SDEP), DESA Charter, and Framework Participation Agreement (PCPP).

Scope of Immunity. Staff designated under official rosters and notified to the Host State shall enjoy immunity from legal process in respect of words spoken or written and acts performed in their official capacity, consistent with Article 31 of the Vienna Convention on Diplomatic Relations (1961), adapted for functional application. Immunity does not extend to private commercial transactions, civil actions unrelated to official functions, or criminal acts outside the scope of duty. Immunities shall not impede cooperation with legitimate investigations into corruption, fraud, or gross misconduct; waiver mechanisms are embedded under Document 11 (Compliance Code) and exercised by the governing body upon prima facie evidence.

Taxation and Social Security. Staff remunerations may be exempt from direct taxation in the Host State where provided by the Host Country Agreement, subject to reciprocity and disclosure obligations. Social security contributions shall follow either the Host State regime or an agreed alternative scheme, documented in annexes to the Host Country Agreement. Exemptions shall not be construed to permit avoidance of obligations under international anti-money-laundering norms or domestic reporting requirements.

Privileges Ancillary to Immunity. Staff shall enjoy inviolability of official papers and documents, secure communications (including encrypted digital channels), and freedom of movement within the Host State for official purposes. Digital communications shall comply with GDPR and security baselines under ISO/IEC 27001, enforced through Microsoft enterprise controls (Entra ID, Purview, Defender, Sentinel), mapped to NIST CSF 2.0 and SP 800-207.

Limitations and Waivers. Immunities shall not shield staff from internal disciplinary measures, fiduciary accountability, or external audit obligations under Document 09 (External Validation). Waiver of immunity may be granted where retention would obstruct justice and where waiver does not prejudice

program integrity. All waivers are documented, disclosed in the Transparency Register (Document 13, Chapter 5), and notified to the Host State.

Chapter 2 – Asset Protection

Assets dedicated to Creativa programs—including funds, property, equipment, and digital infrastructure—shall enjoy protection against requisition, seizure, or interference by the Host State or third parties, except under narrowly defined circumstances consistent with international law and the Host Country Agreement.

Inviolability of Premises and Archives. Premises used for official purposes shall be inviolable, subject to security and safety inspections agreed in advance and conducted without prejudice to operational continuity. Archives and official records, whether physical or digital, shall be immune from search or seizure, with digital protections enforced under ISO/IEC 27001 and zero-trust architecture mapped to NIST CSF 2.0/SP 800-207. Encryption standards shall meet or exceed industry norms, with key management governed by Microsoft security stack (Entra ID, Purview, Defender).

Financial Assets. Funds allocated to programs shall be immune from freezing or attachment, except pursuant to judicial orders arising from final judgments in matters unrelated to official functions and subject to prior consultation with the governing body. Banking arrangements shall comply with anti-money-laundering and counter-terrorist-financing norms under FATF Recommendations and internal controls aligned with COSO and IIA IPPF. Governance allocations to GSEA (Document 13, Chapter 2) shall be ring-fenced and disclosed in the Transparency Register.

Movable Property and Equipment. Official vehicles, ICT hardware, and other movable assets shall be exempt from customs duties and taxes where provided by the Host Country Agreement, subject to inventory controls and sustainable procurement standards under ISO 20400. Disposal of assets shall follow documented protocols ensuring value-for-money and environmental compliance under ISO 14001 and occupational safety under ISO 45001.

Digital Infrastructure and Cloud Assets. Cloud environments hosting official data shall be treated as extensions of inviolable archives. Access shall be restricted to authorized personnel under least-privilege principles, enforced through conditional access policies in Microsoft Entra ID and monitored via Microsoft Sentinel. Data residency and sovereignty clauses shall be embedded in Host Country Agreements, ensuring compliance with GDPR and relevant local data-protection laws.

Exceptions and Remedies. Asset protection shall not preclude lawful enforcement actions against private contractors or vendors engaged by Creativa entities, provided such actions do not impair official archives or program continuity. Disputes regarding asset protection shall be resolved under the dispute-resolution mechanisms in the Host Country Agreement, with escalation to arbitration under UNCITRAL Rules where amicable settlement fails.

Chapter 3 – Comparative Treatments

This Policy adopts a functional-immunities baseline calibrated to the operational needs of Creativa Center ecosystem entities while preserving transparency, accountability, and host-state comity. It is intentionally less than full diplomatic status, aligning instead with comparative public-international-law treatments for international organizations and specialized agencies, and with the fiscal and administrative accommodations commonly accorded to development institutions.

Under the Vienna Convention on Diplomatic Relations (1961), diplomatic agents enjoy personal inviolability and broad immunities; that regime is distinct from the functional immunities typically granted to international organizations under the Convention on the Privileges and Immunities of the United Nations (1946) and the Convention on the Privileges and Immunities of the Specialized Agencies (1947), which protect acts performed in an official capacity, inviolability of archives, and certain fiscal facilities. International financial institutions, including the World Bank Group and the IMF, are accorded immunities for archives, assets, and official acts under their founding instruments (e.g., IBRD Articles of Agreement, Article VII; IDA Articles of Agreement, Article VIII; IMF Articles of Agreement), reflecting a balance between independence and oversight. Within the European Union, organs and agents benefit from a tailored privileges regime under Protocol No 7 on the Privileges and Immunities of the European Union, again emphasizing functional necessity rather than personal immunity. The Council of Europe General Agreement on Privileges and Immunities (1949) similarly codifies archives' inviolability, fiscal relief, and protections necessary for official work.

Against this backdrop, Creativa's approach is precise. First, staff immunities are functional, protecting official acts and records while excluding private transactions or criminal conduct beyond duty, in line with UN-family conventions. Second, asset protection adheres to the organizational model: inviolability of archives (including cloud-based records), protection of funds used for official purposes, and controlled customs/tax facilities where negotiated. Third, waiver practice is structured: immunity may be waived when retention would obstruct justice and when waiver does not prejudice program integrity, consistent with comparative practice under UN conventions and IFI articles. Fourth, dispute resolution follows neutral fora, ordinarily under UNCITRAL Arbitration Rules, ensuring judicial review substitutes where domestic courts are not available due to immunity.

This chapter constitutes the overarching bare minimum that applies across the Creativa ecosystem. Each component—e.g., SUDESA, DESA units, PCPP, PCGG institutions (GSCA components), GSIA, GSEA, GSDA, CGSA/SLUC/Agenda 2074, WOSL Group—shall adopt its own privileges and compliance policies, negotiated in component-specific annexes to Host Country Agreements and framework instruments. Those annexes may strengthen or refine protections to match sectoral risk, fiduciary exposure, or operational footprint, but may not dilute baseline safeguards, anti-corruption controls, or digital-trust duties set in this Policy, Document 11 (Compliance Code), and Document 12 (Data Protection & Digital Trust Policy). All component-level adaptations must remain compatible with responsible business conduct under the OECD Guidelines for Multinational Enterprises (2023) and human-rights due diligence per the UN Guiding Principles on Business and Human Rights.

Chapter 4 – Host Country Agreement Provisions

The Host Country Agreement (HCA) is the constitutive instrument that recognizes the legal personality of the relevant Creativa entity in the host jurisdiction and operationalizes functional immunities, asset protection, and administrative facilities necessary for program delivery. The following provisions represent baseline clauses, to be supplemented by component-specific schedules for SUDESA, DESA units, PCPP programs, and PCGG/GSCA/GSIA/GSEA bodies.

The HCA shall first recognize legal personality and capacity to contract, acquire property, and litigate or be party to arbitration in accordance with agreed dispute mechanisms, ordinarily the UNCITRAL Arbitration Rules. It shall then delineate functional immunities for acts performed in official capacity, including inviolability of archives and official communications, constrained by explicit waiver procedures exercisable by the governing body upon prima facie evidence of corruption, fraud, or serious misconduct, with cross-reference to Document 11 (Compliance Code) and Document 09

(External Validation & Peer Review Protocol). Asset protection clauses shall confirm inviolability of premises used for official purposes, protection of funds and financial assets used in the discharge of mandates, and customs/tax facilities for official imports, subject to inventory and sustainable procurement duties consistent with ISO 20400 Sustainable Procurement.

The HCA must codify digital inviolability of official records, including cloud-hosted archives, with identity, access, retention, and monitoring controls aligned to GDPR, ISO/IEC 27001, and zero-trust architecture under the NIST Cybersecurity Framework 2.0 and NIST SP 800-207. Enforcement shall be supported by Microsoft enterprise controls for identity, data governance, endpoint and threat protection, and security analytics (Entra ID; Microsoft Purview; Microsoft Intune; Microsoft Defender; Microsoft Sentinel). Data residency terms shall specify lawful storage locations and cross-border transfer mechanisms, with audit trails discoverable for external assurance and donor inspections.

Fiscal and administrative facilities shall be narrowly tailored. Tax and customs relief apply to official purchases and imports needed for program delivery; resale or private use is prohibited. Migration and movement provisions shall facilitate visas and residence permits for designated staff and experts on official duty, without derogating from national security or public health measures. Financial operations shall assure free transfer and convertibility of funds used for official purposes, subject to compliance with FATF Recommendations and domestic AML/CFT law, and with internal controls aligned to COSO Internal Control and internal audit under the IIA IPPF.

To entrench transparency and accountability, the HCA shall mandate adherence to the Financial Transparency Register (Document 13, Chapter 5), including disclosure of funding sources, procurement outcomes, and assurance opinions, with climate-related claims positioned for external assurance under ISAE 3410 and program assurance under ISAE 3000 (Revised). Anti-corruption, compliance, and whistleblowing provisions shall require systems conformant with ISO 37001, ISO 37301, and ISO 37002, and shall incorporate sanctions screening and conflict-of-interest regimes for staff and vendors.

Crucially, the HCA will include a Governance Allocation clause authorizing a capped, non-operational compliance allocation to GSEA for custodial oversight and external validation, as established in Document 13 (Chapter 2). It will also incorporate remedies and step-in rights calibrated to maintain continuity of essential services: verified corruption, material ESG failure, or systemic data-protection breach may trigger corrective action plans under Document 06 (ESG Safeguards), suspension or re-sequencing under Document 20 (Implementation Roadmap), and, failing cure, termination with orderly asset disposition that preserves archives' inviolability and protects beneficiaries.

Finally, the HCA shall expressly provide that each Creativa component operates under its own privileges and compliance policies, appended as component-specific schedules or annexes. Those annexes may grant additional narrowly tailored facilities proportionate to the component's risk profile (e.g., field-security for SUDESA; procurement modalities for DESA; cross-border data-sharing for PCPP), provided they remain compatible with this Policy, responsible business conduct under the OECD Guidelines (2023), and human-rights due diligence per the UNGPs.