NOVEMBER 7, 2025

DATA PROTECTION AND DIGITAL TRUST POLICY

PRIVACY AND SOVEREIGNTY SAFEGUARDS, ZERO-TRUST SECURITY, IDENTITY GOVERNANCE, LOGGING AND AUDITABILITY, AND MICROSOFT ECOSYSTEM INTEGRATION

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Data Protection and Digital Trust Policy

Preamble

This Policy codifies privacy, data sovereignty, and digital-trust requirements for all GSEA/SLUC operations and Components, including DESA's digitalisation functions. It harmonises legal, ethical, and technical controls to protect personal and sensitive data, ensure defensible security, and sustain public-interest transparency. The Policy aligns with the EU General Data Protection Regulation (GDPR), cloud-privacy and security standards (ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27018, ISO/IEC 27017), and risk frameworks including NIST Cybersecurity Framework (CSF) 2.0 and NIST SP 800-207 (Zero Trust). Cross-border transfers follow EU Standard Contractual Clauses (SCCs) or equivalent safeguards, and regional sovereignty obligations (e.g., AU Malabo Convention) are respected.

Chapter 1 — Privacy and Sovereignty Principles

1.1 Lawfulness, Fairness, Transparency.

All personal-data processing must specify lawful bases, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability, in line with GDPR Articles 5–6. Privacy notices shall be concise, intelligible, and accessible.

1.2 Privacy-by-Design and Default.

Projects must embed privacy impact analysis at design stage and default to the least-privilege, least-data posture, with Data Protection Impact Assessments (DPIAs) where risk is high (GDPR Arts. 25, 35).

1.3 Data Sovereignty and Localisation.

Hosting and processing arrangements must comply with applicable sovereignty or localisation laws. For international transfers of EU-origin data, adequacy decisions or SCCs are required; transfer-impact assessments must consider destination-country surveillance and redress regimes.

1.4 Special-Category and Sensitive Data.

Processing of special categories (health, biometrics, etc.) requires explicit consent or other lawful grounds and enhanced security; de-identification and aggregation are mandatory for public reporting.

1.5 Community and Indigenous Data.

Where community or Indigenous data are implicated, FAIR principles are complemented by CARE (Collective Benefit, Authority to Control, Responsibility, Ethics), with governance agreements that recognise authority to control and culturally appropriate consent.

1.6 Rights of Data Subjects.

Mechanisms shall provide access, rectification, erasure, restriction, portability, and objection rights, with timelines meeting GDPR standards and secure identity verification.

Chapter 2 — Security Architecture

2.1 Defence-in-Depth and Zero Trust.

Security architecture adopts a defence-in-depth posture and Zero Trust design: verify explicitly, use least privilege, and assume breach. Network micro-segmentation, continuous verification, and secure access service edge (SASE) patterns are required for distributed operations.

2.2 Governance, Risk, and Compliance.
An Information Security Management System (ISMS) aligned with ISO/IEC 27001 governs policy, risk assessment, treatment, and continuous improvement; privacy governance aligns with ISO/IEC 27701. Control baselines may draw from NIST CSF 2.0 functions (Identify-Protect-Detect-Respond-Recover) and mappings to ISO/IEC 27002 where applicable.

2.3 Cryptography and Key Management.
Data in transit shall use modern TLS (e.g., TLS 1.3) and in-rest encryption shall be mandatory for sensitive datasets. Key management adopts segregation of duties, HSMs where proportionate, rotation, and revocation procedures consistent with ISMS requirements.

2.4 Cloud and SaaS Controls.
Cloud deployments adopt shared-responsibility models and control sets reflecting ISO/IEC 27017 (cloud security) and ISO/IEC 27018 (PII in public cloud), including tenant isolation, secure configuration baselines, and continuous posture management.

2.5 Vulnerability, Patch, and Threat Management.
A continuous vulnerability management programme shall operate with defined SLAs for critical patches, authenticated scanning, threat-intelligence ingestion, and red-/purple-team exercises proportionate to risk. Incident handling aligns with ISO/IEC 27035 and recovery with ISO 22301.

2.6 Monitoring and Anomaly Detection.
Centralised logging and security analytics (SIEM/SOAR) provide behavioural analytics, UEBA, and detections mapped to the enterprise risk register. Telemetry retention and tamper-evident storage support forensic readiness and legal hold.

2.7 Third-Party and Supply-Chain Security.
Suppliers are risk-assessed against contractual security clauses, right-to-audit, breach-notification timelines, and data-handling requirements; independent certifications (e.g., ISO/IEC 27001) are reviewed but not deemed sufficient without evidence of effective operation.

Chapter 3 — Identity and Access Management

Identity and Access Management (IAM) is established as a Zero-Trust-aligned control domain enforcing strong, adaptive authentication, least-privilege authorisation, and continuous access verification across all platforms. IAM policies implement role-based and, where warranted, attribute-based authorisation, with segregation of duties enforced for privileged operations. Authentication leverages phishing-resistant multi-factor methods (e.g., FIDO2/WebAuthn security keys) consistent with NIST SP 800-63 Digital Identity Guidelines and integrated with the organisation's federated identity provider (NIST 800-63; FIDO/WebAuthn). Privileged Access Management (PAM) requires dedicated admin identities, just-in-time elevation, session recording, and vaulted secrets with rotation and revocation workflows. Joiner-Mover-Leaver processes automate provisioning and de-provisioning, with periodic access recertification for high-risk systems.

IAM technical and procedural controls are embedded within the ISMS in alignment with ISO/IEC 27001 and the control guidance of ISO/IEC 27002 and mapped to NIST CSF 2.0 functions (Identify, Protect, Detect, Respond, Recover) (ISO/IEC 27002; NIST CSF 2.0). Access to special-category data requires step-up authentication and explicit data-processing authorisations under GDPR. Machine-to-machine identities (service principals, workloads) follow the same least-privilege and rotation imperatives, with mutual TLS and managed identities preferred over long-lived credentials.

Chapter 4 — Logging and Audit Trails

The Group shall operate comprehensive, tamper-evident logging and audit trails to support accountability, forensic readiness, and regulatory reporting. Logging policies define required events across identity, access, administrative changes, data creation/alteration/deletion, security alerts, and data-exfiltration attempts. Time synchronisation is enforced organisation-wide; logs are centrally collected in a SIEM, retained per risk-based schedules, and protected with immutability controls. Analytical use cases include user and entity behaviour analytics, correlation with threat intelligence, and automated response playbooks (SOAR). Design and operation follow NIST SP 800-92 – Guide to Computer Security Log Management and ISO/IEC 27002 logging controls; incident processes align with ISO/IEC 27035 and recovery with ISO 22301 (NIST 800-92; ISO/IEC 27035; ISO 22301).

Where logs may contain personal data, the principles of minimisation, purpose limitation, and retention control under GDPR apply; pseudonymisation and role-based disclosure protect privacy during investigations (GDPR). Cross-border transfer of telemetry follows the same international-transfer rules as production data, relying on adequacy, Standard Contractual Clauses (SCCs), and documented transfer-impact assessments (EU SCCs). Access to audit trails by internal audit, compliance, and accredited validators is logged, justified, and periodically reviewed. High-risk systems adopt write-once, read-many (WORM) or equivalent immutability, with cryptographic integrity proofs.

Chapter 5 — Microsoft Ecosystem Integration

To operationalise privacy, security, and digital trust at scale, SLUC and GSEA shall implement the Policy through Microsoft's enterprise stack, leveraging existing Microsoft 365 (E5) entitlements and Azure services. Identity and Zero-Trust enforcement rely on Microsoft Entra ID (Conditional Access, Authentication Strengths, Identity Protection, Privileged Identity Management, Access Reviews, Entitlement Management), enforcing phishing-resistant MFA and least-privilege access with continuous risk evaluation. Device and application governance is delivered via Microsoft Intune for endpoint compliance and app protection, integrated with Conditional Access for real-time policy decisions.

Information protection and regulatory compliance are implemented through Microsoft Purview: sensitivity labels and encryption (including Double Key Encryption for sovereign scenarios), Data Loss Prevention, Records Management, eDiscovery, Insider Risk Management, and the Compliance Manager control library for continuous assessment. Data residency and sovereignty are supported by Microsoft 365 Multi-Geo and the EU Data Boundary options where applicable; for additional cryptographic control, Customer Key is enabled for Exchange Online, SharePoint, and OneDrive workloads.

Threat protection and SOC operations are anchored in Microsoft Defender XDR (Defender for Endpoint, Office 365, Identity, and Cloud Apps) feeding Microsoft Sentinel as the cloud-native SIEM/SOAR. Cloud posture and workload protection are managed through Microsoft Defender for Cloud, integrated with Azure Policy and landing-zone blueprints to enforce compliance at scale. For highly sensitive processing, Azure Confidential Computing options are evaluated to preserve data confidentiality in use.

Auditability is preserved by enabling Microsoft Purview Audit (Standard/Premium) and forwarding high-value logs to Sentinel for immutability and advanced analytics. Privacy workflows, subject-rights fulfillment, and data-map visibility may be further strengthened with Microsoft Priva. Integration design must respect shared-responsibility boundaries, document data-flow maps, and ensure that all

telemetry subject to GDPR follows the same retention and international-transfer safeguards as production data.