NOVEMBER 5, 2025

DATA PROTECTION AND DIGITAL TRUST POLICY

Safeguarding Sovereignty and Privacy through Secure Digital Architecture and Trusted Ecosystem Integration

CREATED BY

EUSL AB
Care to Change the World

Table of Contents

Data Protection and Digital Trust Policy

Chapter 1 — Privacy and Sovereignty Principles

Preamble to Document 12 and Chapter 1. This Policy is promulgated under the GSIA Charter and shall be read consistently with Documents 00–11 and the prevalence order previously affirmed. It articulates the principles governing privacy, data sovereignty, and digital trust for GSIA-mandated programmes, GSIA AB operations under SLA, GSIA Holding AB stewardship repositories, and Hosted Ownership portfolios operated through EUSL or other approved SPVs. Publication remains a control with lawful, time-limited exceptions by reasoned resolution. Fiduciary controls (four-eyes, segregation of duties, countersignature thresholds, discrete ledgers and bank accounts) apply to data-driven processes where value, rights, or eligibility decisions are affected. Domestication gates govern staged transfer of systems and data stewardship to public custodians. Hosted Ownership is ring-fenced, subject to non-attachment, negative pledge, discrete ledgers and bank accounts, and a reversion covenant without private distribution of value.

1.1 Constitutional Allocation of Roles. The controller for public-interest processing is ordinarily the GSIA SCE or the competent Member authority designated in the governing instrument; GSIA AB and engaged vendors act as processors bound by a Data Processing Agreement. GSIA Holding AB is steward of canonical data models, taxonomies, and method libraries and may act as joint controller where stewardship repositories contain personal data necessary to the public mandate, as determined by reasoned resolution with a defined purpose, minimisation parameters, and publication constraints.

1.2 Lawfulness, Purpose Limitation, and Minimisation. All processing of personal data must rest on a documented lawful basis appropriate to the jurisdiction and instrument, limited to specified, explicit, and legitimate purposes connected to programme delivery, assurance, MEL, fiduciary controls, ESG safeguards, investigations, or statutory duties. Data collection is proportionate and minimised to what is necessary for those purposes. Secondary use is prohibited absent a fresh lawful basis and compatibility assessment approved by reasoned resolution and recorded in the publication register.

1.3 Sovereignty and Localisation. Sovereign prerogatives over public data are respected. Where national law mandates localisation of certain datasets, processing is architected to ensure in-country storage and primary processing, with cross-border access limited to metadata or de-identified artefacts unless a lawful transfer mechanism is in place. Evidence escrow and notarised integrity artefacts (hashes, timestamps) preserve external verifiability without exporting raw personal data when prohibited. Localisation does not derogate from chain-of-custody, audit, or publication doctrines; rather, those controls are adapted to domestic legal frameworks.

1.4 DPIAs and High-Risk Processing. Data Protection Impact Assessments are mandatory for high-risk processing, including large-scale or systematic monitoring; processing of special categories of data; deployment of new or substantially changed technologies; cross-border transfers from localisation jurisdictions; and processing integral to eligibility decisions, sanctions, or investigations. DPIAs record purposes, lawful bases, necessity and proportionality, risks to rights and freedoms, mitigations, and residual risk acceptance by the controller. Where required by national law, prior consultation with supervisory authorities is undertaken.

1.5 Identity, Access, and Accountability. Identity and Access Management is role-based and enforces least-privilege and multi-factor authentication for privileged roles. Access decisions are traceable to named controllers' delegates; approvals are time-limited and reviewed periodically. Privileged access employs break-glass procedures with immutable logging and post-event review. Segregation of duties prevents single-point manipulation of data that affects entitlements, payments, or public reporting.

1.6 Data Quality, Integrity, and MEL Interface. Data must be accurate, complete, and kept up to date where necessary. Quality controls include input validation, dual-capture for critical identifiers, reconciliations, and periodic verification against authoritative sources. For MEL datasets, indicator definitions, sampling frames, and transformations are documented; lineage metadata and chain-of-custody are preserved. Corrections follow reasoned procedures, with prior values accessible for audit and published in aggregate where appropriate.

1.7 Security by Design and Encryption. Security is embedded by design and by default in systems, datasets, and processes. Encryption is mandatory in transit and at rest for personal data and sensitive operational logs, employing sector-appropriate algorithms and key management. Secure coding, vulnerability management, change control, and incident response are documented and tested. Backups and replicas meet RPO/RTO targets without relaxing security controls.

1.8 Publication Doctrine and Redaction. Transparency is preserved without compromising privacy. Publications containing or derived from personal data undergo lawful redaction, de-identification, or aggregation, with methodologies documented and reproducible. Where publication is deferred to protect investigations, procurement integrity, or privacy under national law, deferrals are reasoned, time-limited, and recorded with a sunset review.

1.9 Rights of Data Subjects and Due Process. Where applicable law grants rights of access, rectification, erasure, restriction, objection, portability, or review of automated decisions, the controller establishes procedures to honour requests within statutory timelines, subject to lawful limitations for public interest, investigations, or confidentiality. Decisions affecting entitlements or sanctions are accompanied by reasoned notices, with avenues for reconsideration and appeal as provided in Document 09 and Document 11.

1.10 Cross-Border Transfers and Mechanisms. Cross-border transfers occur only under valid legal mechanisms recognised by the source jurisdiction, including adequacy decisions, standard contractual clauses, binding corporate rules, or treaty-based instruments, with supplementary measures where required. Transfer registers record datasets, purposes, recipients, safeguards, and retention. Where transfers are prohibited, evidence escrow and remote attestation methods support external validation without data export.

1.11 Retention, Deletion, and Archiving. Retention schedules are purpose-linked and incorporate statutory and Charter survivals. Deletion is secure, logged, and verifiable; archival preserves integrity and accessibility for audit, investigations, and legal defence while respecting minimisation and storage limitation principles. Special handling applies to investigation and sanction files under Document 11 and to MEL repositories under Document 08.

1.12 Third Parties, Processors, and Sub-Processors. Processors and sub-processors are onboarded under documented DPAs with explicit purpose, security, localisation, incident notification, audit, and publication clauses. Changes in sub-processor lists are notified to the controller with a right to object on reasoned grounds. Processors maintain records of processing, undergo due diligence and periodic audits, and demonstrate compliance through independent attestations or certifications as appropriate.

1.13 Incident Response and Breach Notification. Personal data breaches trigger incident response protocols: containment, assessment, evidence preservation, root-cause analysis, remediation, and communication. Controllers are notified without undue delay; supervisory authorities and affected data subjects are notified within statutory timelines where required. Publications follow the doctrine of transparency with lawful redaction, preserving public trust without compromising security or investigations.

1.14 Domestication and Hosted Ownership Alignment. At shadowing, Member personnel are trained on controller duties, DPIAs, and IAM; at dual-key, joint decisions apply to high-risk processing and cross-border transfers; at lead-role, Members assume day-to-day control over processing with GSIA oversight; at handover and legal localisation, registers, DPAs, and repositories are transferred and adapted to national law; readiness certification confirms effective, lawful, and sustainable data-protection governance. In Hosted Ownership, sovereignty and localisation dictate evidence handling within the ring-fenced perimeter; reversion includes transfer of data and keys with survival of audit and access rights as stipulated.

1.15 Records, Survivals, and Continuous Improvement. Records of processing activities, DPIAs, access decisions, incident logs, publications, deferrals, and data-subject requests are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection duties, audit and access rights, and publication registers. GSIA Holding AB issues periodic updates to models, taxonomies, and control catalogues, reflecting regulatory developments, threats, and lessons learned from audits, validations, and incidents.

Chapter 2 — Security Architecture

2.1 Governance and Separation of Functions. Security architecture is established by resolution of the GSIA SCE and implemented through an authority matrix that separates design, operation, and assurance. GSIA Holding AB maintains the canonical security control framework, reference architectures, baselines, and evidence taxonomies. GSIA AB operates controls within SLA boundaries, with four-eyes approvals and segregation between architecture, operations, and monitoring functions. Independent assurance is provided through Internal Audit, External Audit, and validators and Peer Review Panels under Document 09. Hosted Ownership environments are architected and operated within their ring-fenced perimeters, subject to identical standards adapted to sovereign constraints.

2.2 Principles by Design. The architecture is anchored in defence-in-depth, least-privilege, explicit verification of every access, segmentation and isolation, secure-by-default configurations, data minimisation, and verifiability. Controls are layered to ensure that failure of a single control does not lead to compromise of confidentiality, integrity, or availability. Design decisions are reasoned and recorded; deviations require documented risk acceptance by the controller and time-bound remediation.

2.3 Architectural Layers and Segmentation. Segmentation is enforced across network, workload, application, and data tiers. Network zones separate user, management, and data planes; east-west traffic is restricted by policy. Workloads are grouped by sensitivity and function, with micro-segmentation where risk warrants. Applications are containerised or sandboxed to reduce blast radius. Data is tiered by classification, with distinct storage policies and access patterns. Inter-zone communication is explicitly authorised, logged, and periodically re-validated.

2.4 Cryptography and Key Management. Encryption is mandatory for personal data and sensitive operational logs in transit and at rest, using sector-appropriate algorithms and key lengths. Keys are generated, stored, and used under dual-control and split-knowledge principles, with hardened key-management systems or hardware security modules where feasible. Key lifecycle management includes issuance, rotation, revocation, escrow for lawful recovery, and destruction, with auditable ceremonies and immutable logs. Exceptions require reasoned, time-limited approvals recorded in a cryptographic exception register.

2.5 Logging, Monitoring, and Telemetry. Security-relevant events are logged at system, application, and network layers, time-synchronised to a trusted source, and forwarded to centralised monitoring. Logs are immutable, access-controlled, and retained for the longer of Charter, statutory, or covenant periods. Monitoring incorporates anomaly detection and correlation across identity, data access, configuration drift, and network flows. Alerts are triaged under documented playbooks and escalated per the incident response regime in Document 11.

2.6 Vulnerability and Configuration Management. Authoritative configuration baselines are maintained for all platforms and devices. Vulnerability identification employs continuous scanning and threat intelligence. Remediation timelines are risk-based and reasoned; emergency changes follow expedited but auditable procedures. Configuration drift is detected and corrected; exceptions are recorded with expiry dates and compensating controls. Evidence of remediation, including before-and-after artefacts, is archived and made available for assurance.

2.7 Secure Change and Development Lifecycle. Change management enforces impact assessment, approvals, testing, segregation of duties, and rollback plans. The development lifecycle embeds threat modelling, secure coding practices, code review, and automated testing for vulnerabilities. Supply-chain risk is addressed by verifying provenance of dependencies, maintaining software bills of materials where applicable, and enforcing code-signing and artefact integrity checks. Production releases are signed, verified, and documented.

2.8 Cloud and Multi-Tenant Controls. Where cloud services are used, responsibilities are mapped under a shared-responsibility model. Tenant isolation is enforced through dedicated subscriptions, projects, or resource groups, with policy-as-code guardrails, immutable baselines, and continuous compliance monitoring. Data locality controls enforce sovereign requirements; cross-region replication adheres to lawful mechanisms and DPIAs. Administrative planes are isolated, with privileged access brokered through controlled jump hosts and just-in-time elevation.

2.9 Endpoint, Mobility, and Edge. Endpoints are hardened according to role-based profiles; device compliance is enforced before granting resource access. Mobile device management controls data leakage, encryption, and app hygiene. Edge and field devices used in programme delivery are risk-assessed, inventoried, and governed by update and attestation policies suitable to their operating context, with secure offline modes where connectivity is intermittent.

2.10 Backup, Recovery, and Resilience. Backups are encrypted, versioned, and stored with logical separation to resist ransomware and insider threats. Restore paths are tested regularly to meet Recovery Point and Recovery Time Objectives set under Document 10. Critical systems for MEL, treasury, identity, and evidence repositories are prioritised. Restoration requires dual-control approvals; post-restore integrity checks are recorded.

2.11 Third-Party and Processor Security. Processors and service providers are bound by documented security obligations proportionate to risk, including minimum technical measures, incident notification, audit rights, and publication clauses. Security attestations or certifications are reviewed; where gaps exist, compensating controls or isolation are imposed. Sub-processor changes require notification and a right to object on reasoned grounds.

2.12 Incident Response and Communications. Security incidents are classified by impact and likelihood; containment, eradication, and recovery steps are executed under runbooks that preserve evidence and chain-of-custody. Communications to controllers, Member authorities, supervisory authorities, and affected parties follow statutory timelines and the publication doctrine, with lawful redaction. Lessons learned are captured in after-action reviews and feed control improvements and training.

2.13 Hosted Ownership Safeguards. Hosted Ownership environments are implemented in separately governed and technically isolated perimeters, with discrete identity directories, key vaults, network segments, and monitoring. Administrative access is restricted to named personnel under dual-control with auditable approvals. Evidence, logs, and keys required for reversion are escrowed and kept up to date. No control in a Hosted Ownership perimeter may depend on shared services that could defeat ring-fencing or negative pledge obligations.

2.14 Domestication Alignment. At shadowing, Member personnel review reference architectures and participate in risk assessments. At dual-key, joint approvals apply to security-relevant changes and privileged access. At lead-role, operating control over security procedures transfers to Member teams under GSIA oversight. At handover and legal localisation, documentation, configurations, keys, and runbooks are transferred, and the architecture is aligned to national standards without diluting core protections. Readiness certification requires evidence of sustained control operation, tested restores, and effective monitoring.

2.15 Publication and Transparency. High-level security architecture summaries, control catalogues, and assurance results are published with lawful redaction; sensitive details that would create exploitable risk are withheld by time-limited, reasoned resolution recorded in the deferral register. Registers of exceptions, key ceremonies, and change approvals are maintained and are accessible to validators and auditors under controlled conditions.

2.16 Records, Survivals, and Interfaces. Architecture decision records, baselines, change logs, scanning results, incident records, and assurance artifacts are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection duties, audit and access rights, and publication registers. This Chapter interfaces with Document 11 for incident response and sanctions, Document 10 for continuity and stress testing, Document 08 for MEL data governance, and Document 07 for DPA and security annex templates.

Chapter 3 — Identity and Access Management

3.1 Mandate and Constitutional Roles. Identity and Access Management (IAM) is a mandatory control framework established by the GSIA SCE to safeguard lawful, proportionate, and auditable access to systems and data. The controller—ordinarily the GSIA SCE or a competent Member authority—owns access policy and approves high-risk access decisions. GSIA Holding AB maintains the canonical IAM control catalogue, model role definitions, and evidence templates. GSIA AB operates IAM under SLA with strict segregation between identity administration, access approvals, and monitoring. Hosted Ownership IAM is operated within separate directories and key stores to preserve ring-fencing.

3.2 Access Models and Role Engineering. Access is granted using role-based models with attribute-based refinements where warranted by sensitivity and purpose. Roles are defined by job function and minimum necessary privileges. Authority matrices align system roles with fiduciary duties, segregation-of-duties constraints, and countersignature thresholds used in treasury, procurement, MEL, investigations, and publication workflows. Role definitions and mappings are version-controlled, reasoned, and reviewed periodically.

3.3 Joiner-Mover-Leaver Lifecycle. Access lifecycle processes are documented and enforced. Joiner processes validate identity, lawful basis, purpose, and manager attestation; temporary access is time-boxed. Mover processes ensure prompt adjustment of privileges when roles change, preserving segregation of duties. Leaver processes enforce immediate revocation of access and retrieval or invalidation of credentials. All lifecycle events are logged immutably and reconciled against HR and contractor records.

3.4 Authentication and Credential Policy. Authentication is proportionate to risk, with multi-factor authentication required for privileged roles and for access to personal data or sensitive operational logs. Credential issuance, rotation, and revocation follow documented procedures; shared credentials are prohibited. Service accounts are minimised, uniquely identified, restricted in scope, and rotated under automated control with dual-control approvals for elevation.

3.5 Authorisation and Least-Privilege Enforcement. Access is granted on a need-to-know basis for defined purposes and durations. Group membership and role assignments are controlled by workflow approvals and are reviewed at defined intervals through access recertifications. Just-in-time elevation is used for administrative tasks, with automatic expiry and session recording. Static standing privileges are discouraged and require reasoned justification and periodic re-approval.

3.6 Privileged Access Management. Privileged accounts are brokered through managed elevation systems that enforce check-in/check-out of credentials, session isolation and recording, command restrictions, and real-time monitoring. Dual approvals are required for elevation to highly privileged roles. Administrative consoles are reachable only through hardened jump hosts in controlled network zones. Break-glass procedures exist for emergencies and require subsequent forensic review and justification.

3.7 Federation, SSO, and Trust Frameworks. Where Single Sign-On or identity federation is established with Member authorities or partners, trust is governed by documented agreements specifying attributes, assurance levels, cryptographic requirements, data minimisation, and incident notification duties. Cross-border federation respects sovereignty and localisation constraints; where attributes originate from onshore systems, they are consumed in ways that avoid unlawful data export.

3.8 Access to Evidence and MEL Repositories. Access to evidence stores, MEL repositories, and investigation case systems is strictly controlled under controller-approved policies, with additional approvals required for special category data. Read-only, time-bound, and audited access is used for validators and auditors. Export controls prevent uncontrolled exfiltration; redaction and de-identification are applied where feasible.

3.9 Monitoring, Analytics, and KRIs. IAM telemetry—authentication events, privilege elevations, access requests, group changes, and anomalous access patterns—is monitored continuously. Key risk indicators include failed authentication spikes, stale privileged accounts, overdue recertifications, excessive privilege accumulation, and unauthorised data access attempts. Breaches of thresholds trigger escalation under Document 17's risk taxonomy and the incident response protocols of Document 11.

3.10 Data-Protection Interfaces and DPIAs. Access to personal data is lawful only where tied to a documented purpose, with the controller's approval recorded. High-risk access patterns—large-scale reads, cross-border access, programmatic extraction—require prior DPIAs and compensating controls. Logs evidencing access to personal data are retained and are available to support data-subject rights and independent assurance.

3.11 Hosted Ownership IAM and Reversion. Hosted Ownership perimeters use separate directories, domain namespaces, and key vaults. Approvals for access in these perimeters are obtained from both the operator and the Member during dual-key domestication; at lead-role, the Member assumes approval authority. Prior to reversion, directory objects, policies, and keys are exported or transferred securely; administrative roles are re-assigned; and all shared pathways are severed. Survival clauses preserve audit access and evidence retention for defined periods post-handover.

3.12 Publication, Registers, and Transparency. IAM policies, role catalogues, recertification schedules, and summaries of privileged access controls are published with lawful redaction. Access registers—covering privileged accounts, emergency access invocations, and material role changes—are maintained and made available to validators and auditors. Deferrals of publication for security are reasoned, time-limited, and entered in the deferral register with a sunset review.

3.13 Records, Survivals, and Interfaces. Identity records, approval workflows, elevation logs, recertification attestations, federation agreements, and incident records are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and publication registers. This Chapter interfaces with Document 11 for sanctions and investigations, Document 10 for continuity of identity services, Document 07 for DPA and security annexes, and Document 08 for MEL data governance.

Chapter 4 — Logging and Audit Trails

4.1 Mandate and Constitutional Role. Logging and audit trails are established as immutable evidence constructs to ensure accountability, verifiability, and forensic readiness across all GSIA-mandated programmes, GSIA AB operations under SLA, GSIA Holding AB stewardship repositories, and Hosted Ownership perimeters. The GSIA SCE mandates logging standards by resolution; GSIA Holding AB maintains canonical taxonomies, retention matrices, and integrity verification methods; GSIA AB operates logging systems under SLA with segregation of duties between generation, storage, and review. Hosted Ownership environments implement identical standards adapted to sovereign constraints.

4.2 Principles and Evidentiary Standards. Logs must be complete, accurate, time-synchronised to a trusted source, and immutable. They constitute primary evidence for assurance, investigations, and dispute resolution. Chain-of-custody is preserved from generation to archival. Any alteration or deletion outside documented retention schedules is prohibited and sanctionable under Document 11 Chapter 4. Exceptions for lawful erasure (e.g., GDPR obligations) require reasoned resolution, documented risk assessment, and compensating integrity artefacts (hashes, notarised inventories).

4.3 Scope of Logging. Mandatory logging domains include:

- **Identity and Access Events:** authentication attempts, privilege elevations, role changes, federation assertions.

- **Data Access and Processing:** reads, writes, exports, and transformations involving personal data or sensitive operational logs.
- **System and Configuration Changes:** deployments, patches, parameter changes, and break-glass invocations.
- **Financial and Fiduciary Actions:** payment approvals, treasury transactions, hedge executions, escrow releases.
- **Evidence Handling:** acquisition, transfer, and review of artefacts in investigations or assurance engagements.
- **Publication and Redaction Decisions:** approvals, reasons, and expiry dates for deferrals.

4.4 Technical Controls and Integrity. Logs are written to append-only stores or WORM (Write Once Read Many) media, cryptographically hashed, and periodically notarised. Time synchronisation uses secure protocols and trusted sources. Access to logs is governed by least-privilege IAM with multi-factor authentication; privileged access requires dual approvals and session recording. Tamper detection alerts are triaged under incident response protocols.

4.5 Monitoring and Analytics. Logs feed centralised monitoring systems for correlation and anomaly detection across identity, data, and network layers. Key risk indicators include unauthorised privilege escalations, repeated failed authentication, configuration drift, and anomalous data access. Breaches trigger escalation under Document 17's risk taxonomy and Document 11's incident response regime.

4.6 Retention and Archiving. Retention periods align with statutory requirements, Charter survivals, and financing covenants, whichever is longer. Archival preserves integrity through cryptographic hashes and notarised inventories. Retrieval processes are documented and tested periodically. Hosted Ownership logs are retained within sovereign boundaries or escrowed under lawful mechanisms, preserving verifiability for reversion and post-handover audit rights.

4.7 Publication and Transparency. High-level summaries of logging standards, retention matrices, and assurance results are published with lawful redaction. Detailed logs are disclosed only under controlled conditions to validators, auditors, or competent authorities. Deferrals for security or investigation sensitivity are reasoned, time-limited, and recorded in the deferral register.

4.8 Domestication Alignment. At shadowing, Member personnel review logging frameworks; at dual-key, joint approvals apply to privileged log access; at lead-role, Members assume operational control of log review and retention; at handover, logging systems and archives are transferred and localised to national law. Readiness certification requires evidence of sustained logging integrity and retrieval capability.

4.9 Records, Survivals, and Interfaces. Logging records, integrity artefacts, retention schedules, and publication registers are archived securely. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP in taxonomies and templates. Interfaces exist with Document 11 for investigations and sanctions, Document 10 for continuity, and Document 07 for DPA annexes.

Chapter 5 — Microsoft Ecosystem Integration (with Future Transition Note)

5.1 Current State and Constitutional Context. GSIA currently operates core productivity, collaboration, and identity services within the Microsoft 365 ecosystem under enterprise licensing, leveraging its compliance certifications (ISO/IEC 27001, 27701, SOC 1/2, GDPR commitments) and integrated security stack. Integration supports IAM, encryption, logging, and conditional access controls aligned with Chapters 2–4 of this Policy. The GSIA SCE mandates configuration standards; GSIA Holding AB maintains canonical mappings between GSIA controls and Microsoft service capabilities; GSIA AB operates tenancy under SLA with segregation of duties and four-eyes approvals for privileged actions.

5.2 GDPR and Schrems II Considerations. The Schrems II judgment and subsequent regulatory guidance have heightened scrutiny of cross-border data transfers to U.S.-based service providers. While Microsoft currently offers EU Data Boundary commitments and contractual safeguards, residual risk remains under evolving interpretations of adequacy and surveillance law. GSIA acknowledges these constraints and applies supplementary measures: encryption with GSIA-controlled keys, pseudonymisation where feasible, and strict IAM with privileged access monitoring. DPIAs document residual risks and mitigations; lawful transfer mechanisms (e.g., SCCs) are maintained and reviewed periodically.

5.3 Future Transition Strategy. GSIA recognises that several jurisdictions, including Germany and other EU Member States, are actively developing sovereign cloud and productivity alternatives designed to meet GDPR and Schrems II compliance without reliance on U.S.-based processors. GSIA's roadmap includes phased evaluation and migration to such alternatives when they achieve functional parity and certification benchmarks. Transition planning will be reasoned, documented, and published, with domestication gates adapted to ensure continuity and readiness certification. Until viable alternatives are operational, Microsoft remains the default ecosystem under enhanced safeguards.

5.4 Integration Controls and Assurance. Current integration enforces:

- Conditional Access policies tied to risk signals and device compliance.
- Multi-factor authentication for all privileged roles.
- Privileged Access Management with just-in-time elevation and session recording.
- Encryption in transit and at rest, with GSIA-controlled keys for sensitive workloads where supported.
- Immutable logging of administrative actions and data access events, exported to GSIA-controlled archives for assurance.
- Data-loss prevention and information protection labels aligned to GSIA classification schema.

Evidence of control operation is preserved and made available for internal and external assurance engagements under Document 09.

5.5 Hosted Ownership and Sovereignty. For Hosted Ownership perimeters, Microsoft tenancy is logically segregated through dedicated subscriptions, resource groups, and conditional access constructs. Data localisation commitments are enforced to the extent supported by Microsoft EU Data Boundary features. Escrowed artefacts (keys, logs, configurations) ensure verifiability and continuity for reversion. No Hosted Ownership perimeter may depend on shared administrative pathways that could defeat ring-fencing or negative pledge obligations.

5.6 Domestication and Transition Alignment. At shadowing, Member personnel are trained on Microsoft tenancy governance; at dual-key, joint approvals apply to privileged actions; at lead-role, Members assume operational control under GSIA oversight; at handover, tenancy or its successor platform is transferred and localised to national law. Transition to alternative ecosystems will follow the same domestication logic, with readiness certification contingent on demonstrated compliance with GDPR, Schrems II jurisprudence, and GSIA standards.

5.7 Publication and Registers. Integration standards, DPIA summaries, and transition roadmaps are published with lawful redaction. Deferrals for security or procurement sensitivity are reasoned, time-limited, and recorded in the deferral register. A Transition Register tracks milestones, dependencies, and readiness indicators for migration to sovereign alternatives.

5.8 Records, Survivals, and Continuous Improvement. Configuration baselines, access logs, DPIAs, contractual safeguards, and transition planning documents are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP in mappings and templates. GSIA Holding AB issues periodic updates to integration standards and transition guidance based on regulatory developments and market maturity of alternatives.

References

Microsoft EU Data Boundary and Schrems II Context

- Microsoft EU Data Boundary Overview – Microsoft Trust Center – Official documentation on Microsoft's EU Data Boundary commitments, technical measures, and transparency resources. [microsoft.com]
- Schrems II and Microsoft – Legal and Compliance Measures – Explains Microsoft's use of SCCs and supplementary measures post-Schrems II. [iia.no]
- Microsoft Completes EU Data Boundary – TechTimes – Details on Microsoft's localization strategy and sovereign cloud initiatives. [techtimes.com]
- European Data Protection Board (EDPB) Recommendations on Schrems II – Official guidance on supplementary measures for international transfers. [edpb.europa.eu]

ISO Standards for Privacy and Security

- ISO/IEC 27701:2025 – Privacy Information Management Systems – Official ISO page for the updated privacy standard, now standalone. [iso.org]
- ISO/IEC 27001 Overview – Information Security Management – Core standard for ISMS and security architecture alignment. [iso.org]

EU Sovereign Cloud Alternatives

- Gaia-X Official Site – Federated Secure Data Infrastructure – European initiative for sovereign cloud and data spaces, relevant for future transition planning. [gaia-x.eu]
- German Federal Ministry – Gaia-X Ecosystem – Policy and funding framework for Gaia-X and sovereign cloud projects. [bundeswirt...sterium.de]