# Module 23 – Privacy & Sovereign Data Control Capsule

Version: 4.1 | Classification: Sovereign Privacy Enforcement Layer  
Scope: Structural implementation of privacy, consent, and sovereign data control mechanisms within MaxOneOpen Capsule Logic.

**Capsule Initialization**

This capsule is instantiated at runtime whenever user-specific or sovereign-classified data is accessed, modified, or routed through execution layers that require consent lineage, privacy validation, or regulatory enforcement. Capsule validation is enforced before any data processing event and triggers audit-bound execution framing.

**0. Purpose & Design Premise**

This capsule introduces runtime-verifiable privacy controls into the MaxOneOpen architecture. It enforces data sovereignty, purpose limitation, and consent-governed access paths without reliance on centralized brokers or vendor-specific components. Activation is non-optional for all capsules dealing with user or jurisdiction-bound data.

**1. Privacy by Design – Runtime Layer**

- All data access paths are capsule-enforced and policy-bound.

- Purpose declarations are embedded at the point of data invocation.

- Runtime execution carries lineage metadata reflecting privacy scope.

- No capsule may override declared consent logic without authorized escalation trigger.

**2. Consent Handling & Enforcement**

- Consent artifacts are embedded as immutable runtime conditions (CRC-anchored).

- Revocation triggers isolate runtime operations in real-time.

- Consent tiers (default, extended, federation) are structurally enforced through capsule templates.

**3. Data Classification & Sovereignty Logic**

- Supports multi-tier data classification (public, restricted, critical, sovereign).

- Sovereign-classified data declares geographic, legal, and contractual execution bounds.

- Federated capsules enforce execution location compliance (e.g. EU-only).

**4. Compliance Anchors & Regulatory Mapping**

- Capsule logic is mapped to GDPR Articles 5, 6, 25, and 32.

- Regional sub-capsules enable CCPA, LGPD, and other jurisdictional variants.

- All runtime data flows are auditable and exportable via runtime snapshot interface.

**5. Capsule Invocation Controls**

- No data path bypasses privacy capsule validation.

- Audit logs indicate all invocation and enforcement actions.

- Failed validation results in runtime abort with immutable trace state.

**6. Interoperability & Federation Handling**

- Privacy capsules are federated, not delegated.

- Federation participants inherit full enforcement logic.

- Forks must re-certify privacy capsule alignment before runtime admission.

**7. Roadmap Commitments (v4.2 aligned)**

- Predictive anomaly detection via ML-enhanced privacy simulation.

- Zero-knowledge capsule invocation for consent validation.

- Dynamic regional capsule templates for multi-jurisdictional enforcement.

**Final CTO Statement**

This capsule enforces sovereign-grade privacy boundaries with full runtime traceability. It is mandatory for all MaxOneOpen deployments interacting with sensitive, classified, or jurisdiction-bound data. Absence or failure of this capsule renders the runtime non-compliant under v4.1 governance rules.