CDMC Structure – Key Controls

Data Consumption Purpose must be provided for all Data Sharing Agreements involving sensitive data — **8**

Appropriate **Security Controls** must be enabled for sensitive data and evidence must be recorded — **9**

Data Protection Impact Assessments must be automatically triggered for all personal data according to its jurisdiction — **10**

Entitlements and Access for Sensitive Data must default to creator and owner and access must be tracked for all sensitive data — **7**

Data Retention, **Archiving and Purging** must be managed according to a defined retention schedule — **11**

Classification must be automated for all data at the point of creation or ingestion and must be always on — **6**

Data Quality Measurement must be enabled for sensitive data with metrics distributed when available — **12**

Cataloguing must be automated for all data at the point of creation or ingestion, with consistency across all environments — **5**

Cost Metrics directly associated with data use, storage and movement must be available in the catalog — **13**

The **Data Sovereignty and Cross-Border Movement** of sensitive data must be recorded, auditable and controlled according to defined policy — **4**

Data Lineage information must be available for all sensitive data — **14**

A register of **Authoritative Data Sources and Provisioning Points** must be populated for all data assets containing sensitive data — **3**

The **Ownership field** in a data catalog must be populated for all sensitive data or otherwise reported to a defined workflow — **2**

Data Control Compliance must be monitored for all data assets containing sensitive data via metrics and automated notifications — **1**

Structure segments
- 1.0 Governance & Accountability
- 2.0 Cataloguing & Classification
- 3.0 Accessibility & Usage
- 4.0 Protection & Privacy
- 5.0 Data Lifecycle
- 6.0 Data & Technical Architecture