CDMC - Cloud Data Management Capabilities
14 Key Controls & Automations for Managing Sensitive Data

(Click here to access the technical specification)

Sensitive Data includes classifications such as:
- Personal Information **(PI)** / Sensitive Personal Data
- Personally Identifiable Information **(PII)**
- Personal Health Information **(PHI)**
- Company or Client Identifiable Information
- Material Non-Public Information **(MNPI)**
- Specific Information Sensitivity Classifications (such as **'Highly Restricted'** and **'Confidential'**)
- Critical Data Elements used for important business processes
- Licensed data

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

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

Data Privacy Impact Assessments must be automatically triggered for all personal data according to its jurisdiction

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

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

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

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

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

Data Lineage information must be available for all sensitive data

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

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

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

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

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

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

CDMC EDMCouncil — Cloud Data Management Capability