Security & Governance in Salesforce Data Cloud

---

1. Overview

Security and governance are foundational aspects of **Salesforce Data Cloud**, ensuring that all data — from ingestion to activation — is **protected, compliant, and auditable**.

In the **Developer Edition (DE)** environment of Salesforce Data Cloud, you have access to essential **core features** that mirror enterprise-grade controls. These allow administrators to:

- Design secure, role-based access models.
- Protect sensitive data through field-level control and classification.
- Track configuration and administrative changes.
- Implement AI-driven data governance through tagging and policy frameworks.

---

2. Designing Access with Permission Sets and Field-Level Security (FLS)

2.1 Understanding Permission Sets

In Salesforce Data Cloud, **Permission Sets** define **who can access what** — including data objects, fields, and system functions.

Unlike Profiles (which define a user's base access), **Permission Sets are additive**, granting additional permissions without altering a user's profile.

Key Elements

Component	Description
Objects	Define access to DLOs, DMOs, and Unified Objects (read, edit, delete).
Fields	Control access to specific fields (via FLS).
Apps and Tabs	Control access to Data Cloud applications and dashboards.
Administrative Permissions	Grant advanced abilities like Manage Data Cloud Setup or Run Identity Resolution.

2.2 Example: Data Cloud Permission Set Design

Role	Permission Set Name	Access Scope	Key Permissions
Data Engineer	DataCloud_DataOps	Full CRUD on DLOs and DMOs	Manage Data Streams, Run Mapping Jobs
Marketing Analyst	DataCloud_Analytics	Read-only access to Unified Profiles	View Segments, Query CIOs
Admin	DataCloud_Admin	Full access	Manage Rulesets, View Audit Logs
Compliance Officer	DataCloud_Governance	Read-only access to data classification & audit reports	View Data Classification, Audit Trail

2.3 Field-Level Security (FLS)

Field-Level Security (FLS) controls **which users can view or edit individual fields** in an object — even if they have access to the object itself.

FLS is critical for maintaining compliance and minimizing exposure of sensitive attributes such as PII (Personally Identifiable Information).

FLS Examples

Object	**Field**	**FLS Setting**	**Description**
Customer_DMO	email	Read-only for Analysts	Restricts editing of customer PII
Customer_DMO	SSN	Hidden for all except Compliance	Sensitive identifier
Transaction_DMO	amount	Read-only for Marketing	Prevents unauthorized financial edits

---

2.4 Best Practices for Access Design

Best Practice	**Description**
Principle of Least Privilege	Assign only the minimum permissions necessary for a role.
Use Permission Sets over Profiles	Easier to manage and scale in Data Cloud environments.
Separate Roles by Function	Distinguish engineering, analytics, and governance responsibilities.
Enable Field-Level Encryption (where supported)	Protect sensitive attributes at rest.
Review Access Regularly	Use audit logs to detect permission drift.

---

3. Data Classification at Field Level

3.1 Purpose

Data classification allows administrators to **label each field** in Salesforce Data Cloud with **metadata about sensitivity, usage, and compliance requirements**.

This supports privacy laws such as GDPR, CCPA, and HIPAA — and helps teams handle data appropriately across ingestion, processing, and activation.

3.2 Classification Types

Classification Category	**Description**	**Example Tag**
Sensitivity Level	Indicates how confidential the data is	Public, Internal, Confidential, Restricted
Data Type / PII Indicator	Identifies personally identifiable or regulated information	PII, Financial, Health, Non-PII
Compliance Tag	Indicates applicable laws or policies	GDPR, HIPAA, CCPA
Usage Purpose	Describes intended usage	Marketing, Analytics, Service

3.3 Example: Data Classification in a DMO

Field	**Sensitivity**	**Compliance Tag**	**Purpose**	**Description**
email	Restricted	GDPR, CCPA	Marketing	Personally identifiable email address
phone_number	Confidential	GDPR	Service	Contact information
purchase_amount	Internal	PCI	Analytics	Transactional data
city	Public	None	Analytics	Non-sensitive attribute

3.4 Benefits of Data Classification

- Enables **automated policy enforcement** (e.g., prevent activation of PII to ad platforms).
- Supports **data lineage and cataloging**.

- Simplifies **compliance reporting** and **access auditing**.
- Enhances **AI-driven governance and discovery** (auto-tagging sensitive data).

---

4. Viewing Setup Audit Trail

4.1 Purpose

The **Setup Audit Trail** in Salesforce Data Cloud records administrative and configuration changes made in the organization — helping maintain accountability and governance.

It is especially useful for:

- Tracking changes to **Permission Sets**, **Match Rules**, or **Data Streams**.
- Auditing user access modifications.
- Ensuring configuration consistency across environments.

4.2 How to Access the Audit Trail

1. Navigate to **Setup → Security → View Setup Audit Trail**.
2. The log displays up to **6 months** of changes in DE.
3. You can **download the audit log** for deeper analysis.

4.3 Example Audit Trail Log

Date	**User**	**Action**	**Object**	**Description**
2025-10-15	Admin_User	Created	Permission Set	“DataCloud_DataOps”
2025-10-16	DataEngineer	Modified	Data Stream	Updated ingestion mapping

Date	User	Action	Object	Description
2025-10-17	Compliance_Officer	Edited	Classification	Changed “email” sensitivity to Restricted
2025-10-18	Admin_User	Deleted	Ruleset	Removed old Identity Resolution set

4.4 Key Benefits

Benefit	Description
Accountability	Track which admin made what change.
Compliance	Provide change evidence for audits.
Change Control	Detect unauthorized modifications.
Rollback Support	Helps identify configuration errors.

5. Data Cloud Governance Concepts

Salesforce Data Cloud extends traditional data governance into **AI-assisted, policy-driven frameworks** that ensure secure and ethical use of customer data.

5.1 AI Tagging (Automated Data Classification)

Salesforce’s Einstein Trust Layer can **automatically scan and tag data fields** based on content analysis and metadata.

Examples:

- Detects email formats → tags as “PII: Email Address”.
- Identifies numeric account IDs → tags as “Restricted Identifier”.
- Recognizes credit card patterns → tags with “PCI Compliance”.

This supports **data discovery** and reduces manual tagging workload.

5.2 Policy-Based Governance (Reading Only in DE)

In enterprise environments (read-only view in Developer Edition), **Policy-Based Governance** allows administrators to **define rules** that enforce data handling restrictions based on classification tags.

Policy Type	**Description**	**Example Rule**
Access Policy	Restricts user access based on sensitivity	"Restricted fields viewable only by Compliance role."
Usage Policy	Controls data activation or export	"Do not activate PII data to external ad platforms."
Retention Policy	Defines how long data is stored	"Delete customer data after 24 months of inactivity."

Even though DE users can only **view** these capabilities, understanding them is essential for designing compliant Data Cloud architectures.

5.3 Data Governance Benefits

Benefit	**Description**
Improved Data Trust	Ensures data is clean, protected, and compliant.
Operational Transparency	Clear lineage of data transformations and access.
AI-Driven Insights	Automatic tagging and alerting for sensitive data.
Regulatory Readiness	Simplifies GDPR, HIPAA, and CCPA compliance efforts.

6. Example Use Case: Data Governance for a Retail Enterprise

Scenario

A retail enterprise uses Salesforce Data Cloud to unify customer data across CRM, loyalty, and marketing systems.

Challenges

- Sensitive customer PII must be protected from marketing misuse.
- Regulators require auditable logs of admin changes.
- Teams need different access levels (Analyst vs Compliance).

Implementation

Feature	**Configuration**	**Purpose**
Permission Sets	DataCloud_Analytics (Read), DataCloud_Governance (View Classification)	Role-based access control
Field-Level Security	Email and Phone = Restricted	Protect PII
Data Classification	Compliance tags (GDPR, CCPA)	Regulatory compliance
Setup Audit Trail	Daily review by Compliance Officer	Track changes
AI Tagging	Auto-tag new fields based on pattern	Detect sensitive attributes
Policy-Based Governance	Prevent activation of Restricted data	Ensure legal compliance

Outcome

- Zero unauthorized access incidents.
- 100% audit compliance for setup and configuration changes.

- Simplified governance workflows with automated data tagging.

7. Best Practices for Security & Governance in Data Cloud

Area	Best Practice	Description
Access Control	Assign permissions through roles and Permission Sets	Prevent overexposure of data
Field-Level Security	Apply least privilege at field level	Protect sensitive fields
Data Classification	Label all fields upon ingestion	Streamline governance
Audit Logs	Review Setup Audit Trail weekly	Detect anomalies early
AI Tagging	Use auto-classification where available	Reduce manual errors
Governance Policies	Align tags with organizational data policies	Enable compliance automation

8. Summary

Feature	Purpose	Available in DE
Permission Sets & FLS	Manage user and field access	Fully available
Data Classification	Tag fields by sensitivity and compliance	Fully available
Setup Audit Trail	Track admin setup changes	Fully available

Feature	Purpose	Available in DE
AI Tagging & Policy-Based Governance	Intelligent tagging and policy enforcement	View only (Enterprise active)

Key Takeaway

Salesforce Data Cloud’s Developer Edition includes core security and governance features that allow administrators to **design robust access models**, **protect sensitive data**, and **track configuration changes**. Through **data classification**, **field-level controls**, and **audit visibility**, organizations build the foundation of **trust, compliance, and accountability** — even at the prototype or developer stage.