

DATA GOVERNANCE.

The framework of policies, roles, and controls that decide **who can access data, how it's classified, and how long it's kept.** Without governance, a strong security stack still can't answer whether this data should exist.

- DATA CLASSIFICATION
- GDPR / CCPA
- DATA LINEAGE
- RETENTION SCHEDULES

01 THE MECHANISM



Classification & discovery
Automated discovery and tagging find where sensitive data lives and label it — public, internal, confidential, restricted — before any control can be applied.



Ownership & stewardship
Every data domain gets a **named owner and steward** accountable for its quality, access decisions, and lifecycle — governance without an owner is just a policy document.



Policy enforcement
Access controls, retention schedules, and masking rules translate policy into technical enforcement, so the rules hold even when no one is watching.

02 THE FLOW

The Classification Cycle AT CREATION & ON CHANGE

1

New data is **scanned and tagged at creation** using content inspection and contextual rules.

2

The classification sets **default access controls, encryption, and retention** requirements.

3

Reclassification triggers automatically when the data moves, merges, or its context changes.

The Access Request Cycle PER REQUEST

1

A user requests access through a **governed request workflow**, not a direct ask to IT.

2

The data owner or steward **approves, denies, or time-boxes** access based on business need.

3

Access is **logged, reviewed periodically, and automatically revoked** when the need or employment ends.

03 CLASSIFICATION TIERS & HANDLING

TIER	TYPICAL HANDLING
Public	No restrictions — approved for external release as-is.
Internal	Employees and contractors only; not for external sharing.
Confidential	Need-to-know access; encryption at rest and in transit required.
Restricted	Named-individual access only; logged, encrypted, and held to the strictest retention limits.

04 GOVERNANCE SIGNALS COMPARED

CONTROL	SUFFICIENT ALONE?	WHAT IT MISSES
Access Control Lists (ACLs)	No	Says who can access data, not whether it should exist or is classified correctly.
Data Classification Tags	No	Labels sensitivity but doesn't enforce access or retention on its own.
Retention Schedule	No	Governs how long data is kept, not who can see it while it exists.
Data Loss Prevention (DLP)	No	Catches unauthorized movement, but only for data it correctly recognizes as sensitive.
Combined Governance Program (Classification + Ownership + Access + Retention)	Yes	Ties sensitivity, ownership, access, and lifecycle into one accountable, auditable framework.

DATA GOVERNANCE.

CLASSIFY · OWN · ENFORCE

05 PROGRAM OPERATIONS

Data inventory comes before policy.

You can't govern data you haven't mapped, tagged, and assigned an owner to.

Access reviews are recurring, not a one-time project.

Entitlements drift the moment a person changes roles or leaves a team.

Retention is a liability control, not just a checkbox.

Data kept past its useful life is pure legal and breach exposure with no business upside.

Lineage tells you blast radius.

Knowing where data flows lets you scope an incident or deletion request accurately instead of guessing.

06 CONTROL MAPPING

GDPR · CCPA · CPRA

Statutory requirements for **data subject rights**, breach notification, and lawful processing basis.

NIST Privacy Framework

Voluntary framework for identifying and mitigating **privacy risk** across the data lifecycle.

ISO/IEC 27001 Annex A

Information classification and handling controls (**A.5.12**, **A.5.13**, and related).

DAMA-DMBOK

Industry body of knowledge defining **governance**, **stewardship**, and **quality** disciplines.

07 WHAT GOVERNANCE DOES NOT SOLVE

Shadow data & spreadsheets

Ungoverned copies exported to a **local spreadsheet or personal drive** sit entirely outside the program.

Third-party data sharing

Once shared with a vendor or partner, your governance controls **no longer apply** to their environment.

Human judgment at the edge

A steward can still approve access that's **technically compliant but practically unwise**.

Legacy systems without APIs

Systems too old to integrate with discovery and DLP tooling stay **invisible to the program**.

08 MYTHS VS. REALITY

MYTH "Encryption is the same as governance."	REALITY Encryption protects data in transit or at rest, but says nothing about who should have access, why, or for how long.
MYTH "If IT manages access, we don't need a governance program."	REALITY IT enforces the technical control; the business owner still decides who should have access and why.
MYTH "Classifying data once is enough."	REALITY Data changes context as it moves, merges, or ages — classification has to be revisited, not set once.
MYTH "Governance only matters for regulated industries."	REALITY Any organization holding customer, employee, or proprietary data carries breach, legal, and reputational exposure without it.
MYTH "More access controls always mean better governance."	REALITY Overly restrictive controls push employees toward unmanaged workarounds like personal cloud storage.

09 SPEAK THE PROGRAM — KEY TERMS

DATA STEWARD

The individual accountable for a data domain's **quality, classification, and access decisions** day to day.

DATA LINEAGE

The traceable path data takes from its origin through **every system, transformation, and destination** it touches.

DATA CLASSIFICATION

The process of labeling data by sensitivity to determine its **required handling and controls**.

DLP

Data Loss Prevention — tooling that detects and blocks **unauthorized movement** of sensitive data.

RETENTION SCHEDULE

The defined period data must be kept before it must be **deleted or archived**.

DATA SUBJECT RIGHTS

Legal rights — access, deletion, portability — granted to individuals over their **personal data** under laws like GDPR.