Rockin’ Data Privacy – The Rhythm of Governance in a Connected World

Peter Gallinari
Cybersecurity • Data Privacy • Governance

🔐 **Cybersecurity protects systems**
Defends infrastructure and data, detects threats, and enables recovery.

🛡️ **Privacy governs behavior**
Defines responsible data use, accountability, and individual rights.

🧭 **AI Didn’t Fail Us — We Failed AI**
Why Data Governance Must Come Before AI Enablement

🧭 **Governance creates trust**
Establishes ownership, risk decisions, and organizational consistency.

🥁 **Leadership sets the rhythm**
Drives priorities, culture, and sustained execution.

From Compliance to Culture

- **Compliance does not equal accountability**
  Meeting requirements doesn’t ensure responsible action or ownership.
- **Policies fail without ownership**
  Rules only work when roles and decision rights are clearly assigned.
- **Privacy must live in operations**
  Privacy succeeds when embedded into daily workflows, not documents.
- **Security requires discipline**
  Consistent execution matters more than tools or one-time controls.
- **Culture starts at the top**
  Leadership behavior sets expectations the organization follows.

Modern Reality: Distributed Risk

- **APIs move data at machine speed**
  - System-to-system data flows bypass human review
  - Errors and over-permissions propagate instantly
- **Cloud and SaaS expand exposure**
  - Data is distributed across platforms and vendors
  - Shared responsibility often creates accountability gaps
- **Shadow IT becomes Shadow AI (Agentic AI = High Risk)**
  - Employees adopt AI tools outside approved controls
  - Data is used, transformed, or exposed without visibility
- **Vendors sit inside workflows**
  - Third parties are embedded in core business processes
  - Risk is inherited, not outsourced
- **Automation amplifies mistakes**
  - Flawed rules and prompts scale instantly
  - Small errors become enterprise-wide impacts

AI Didn’t Fail Us — We Failed AI

1. Why Data Governance Must Come Before AI Enablement

- AI assumes data ownership, access intent, and classification already exist
- Governance is not optional “cleanup” — it is a prerequisite
- Enabling AI without governance accelerates unmanaged risk

2. AI Inherits Your Environment — Exactly As It Is

- AI does not create new access — it trusts existing permissions
- Identity, roles, and group memberships are taken as truth
- Poor access decisions are amplified, not corrected

3. Governance Is the Missing Control Plane

- Most organizations have not fully audited access entitlements
- Data ownership and accountability are often unclear
- Monitoring focuses on tools, not data usage and behavior

AI Didn’t Fail Us — We Failed AI

4. The SharePoint Reality Check

- Sensitive data exists across **Microsoft SharePoint** environments
- Access reviews are rarely complete or current
- When **Microsoft Copilot** is enabled, exposure becomes instant and scalable

5. Agentic AI Raises the Stakes Even Higher

- AI systems are moving from response to action
- Weak governance becomes operational and compliance risk
- Autonomous workflows assume decisions were already approved

6. Guardrails Only Work After the Foundation Exists

- Guardrails do not fix poor identity or access controls
- Content filters cannot compensate for overexposed data
- Governance maturity determines whether guardrails are effective

Inside-the-Perimeter Risk

- **Excessive user permissions**
  Access accumulates faster than it's removed
  Users can see far more data than required
- **Overexposed APIs**
  APIs are published, reused, and forgotten
  Authentication and scope controls are often too broad
- **Vendor data reuse**
  Data shared for one purpose is reused for others
  Contract terms lag behind technical reality
- **AI surfacing sensitive content**
  AI reveals patterns and data users were never meant to see
  Context and intent controls are missing
- **Most risk is inside the perimeter**
  Insiders, misconfigurations, and automation drive exposure
  Perimeter defenses alone no longer define security

Data Is the Asset — Not the Technology

- **Data Discovery**
  Identify what data exists, where it lives, and how it flows
  Establish visibility across systems, cloud, vendors, and APIs
  You cannot protect or govern what you cannot see

- **Data Classification**
  Define data sensitivity and business value
  Apply consistent labels across platforms and workflows
  Classification drives access, retention, and protection

- **Data Privacy**
  Define how data may be used, shared, and retained
  Protect individual rights and business intent
  Privacy governs behavior — not just compliance

- **Data Security**
  Apply controls based on data risk, not system location
  Enforce least privilege, monitoring, and recovery
  Security protects data — wherever it travels

IT enables and protects data — but the business owns the data, its risk, and its use.

The Governance Rhythm Loop

- **Identify sensitive data**
  Know what data you have and where risk truly exists.
- **Define business purpose**
  Use data only for clear, approved, and justified outcomes.
- **Control access (least privilege)**
  Limit access to only what is necessary to perform the role.
- **Monitor usage and behavior**
  Detect misuse, drift, and risk through continuous visibility.
- **Enforce accountability**
  Hold owners responsible for how data is accessed and used.
- **Recover through DR & BC**
  Ensure data and operations can be restored when disruption occurs.

Disaster Recovery Is Governance

- **Recovery time & recovery point objectives**
  Define how fast systems must recover and how much data loss is acceptable.
- **Backups & failover environments**
  Ensure data and systems can be restored without interruption.
- **Downtime communications**
  Maintain clear, timely communication during outages.
- **Business continuity planning**
  Sustain critical operations through disruption.
- **Executive ownership of resilience**
  Leadership is accountable for recovery readiness.

Resilience isn’t technical readiness alone — it’s leadership accountability.

Real-World Lessons

- **What failed operationally**
  Identify breakdowns in processes, controls, or execution.
- **What leadership assumed**
  Examine assumptions that influenced decisions.
- **Where governance broke**
  Expose gaps in oversight, ownership, or escalation.
- **What changed outcomes**
  Highlight actions that altered impact or recovery.
- **Lessons learned**
  Convert experience into improved controls and decisions.

Incidents don’t define organizations — how they learn does.

Five Leadership Takeaways

- **Embed privacy into security strategy**
  Integrate data protection into security design.
- **Make data ownership explicit**
  Assign clear accountability for data assets.
- **Start AI with governance**
  Establish controls before deploying AI.
- **Vendors inherit your risk**
  Third parties extend your risk posture.
- **Disaster recovery is executive accountability**
  Resilience requires leadership ownership.

Strategy without accountability becomes exposure.

Questions & Discussion

- AI • Privacy • APIs • Vendors • Recovery
- Open discussion

Stay Connected – Rockin Data Privacy

YouTube • Spotify • Articles

Rockin Data Privacy

Rockin Data Privacy | Podcast on Spotify

Rockin Data Privacy - YouTube