USE CASE

Privacy and Compliance

Your Data Has a Passport

Sensitive information is traveling farther, faster, and into more places than ever.

Data moves across departments, applications, partners, and platforms—often far beyond its original purpose. Documents, datasets, and files are copied, shared, modified, and stored across systems. As data crosses regions and regulatory environments, the rules governing how it should be handled can change.

Keeping track of all that data is difficult enough. Keeping it aligned with constantly evolving privacy and compliance requirements is an even larger, more complex challenge.

Security and compliance teams need to know where sensitive data resides, what it contains, how it's used, who has access to it, and where it's going. Without that context, it's difficult to determine whether the right controls are in place—or where compliance gaps may be hiding.

When requirements vary by industry, regulation, or region, compliance can quickly become a moving target.

Compliance Doesn't Travel Well

Visibility breaks down. Sensitive information can be spread across systems, users, and services, making it difficult to maintain a complete picture of where it resides and how it's used.

Context gets lost. Knowing that data is sensitive isn't enough. You need to understand its type, purpose, importance, location, and risk.

Requirements keep changing. Different regulations, industries, and regions have different requirements, and those requirements keep evolving.

Compliance gaps are difficult to investigate. Identifying a problem is only the beginning. Teams need to understand which data, users, services, and activities are behind it so they can make smart decisions about where to act.

You Need a Centralized View

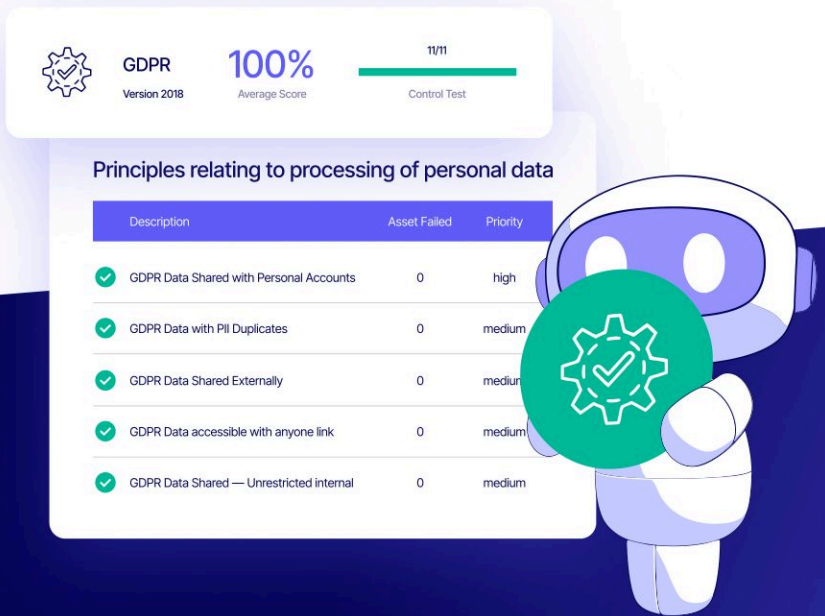
Connect sensitive data and its activity to the requirements that govern it, so you can see where you stand, identify what needs attention, and address issues before they become major problems.

Bring Privacy and Compliance Into Focus

Concentric AI connects sensitive data and its activity to the requirements that govern it, giving security and compliance teams a centralized view of their compliance posture and the context behind it.

The Compliance Dashboard maps your data environment to relevant regulatory and custom frameworks, then lets you drill down from your overall compliance posture to the specific data, users, services, and activity behind areas that need attention.

- **Understand your sensitive data.** Discover sensitive information and identify its sharing activity and access across your environment.
- **Map data to requirements.** Connect your data environment to relevant regulatory frameworks to identify which controls and requirements apply to your organization.
- **Measure and investigate risk.** At a glance, see your compliance posture on the dashboard, then drill into the data, users, services, and activity behind areas needing attention.
- **Take action.** Address violations directly, control access to sensitive data, and automate cleanup based on needs or data retention requirements.



Stay Ahead of Privacy Risk

Better visibility and control help your organization:

Reduce privacy risk by knowing where sensitive information lives, how it moves, and who can access it.

Strengthen compliance with a clear, measurable view of your compliance posture and the areas that require attention.

Control sensitive data by limiting inappropriate access and reducing unnecessary data through better retention and cleanup.

Adapt as your data changes with continuous visibility into data movement, sharing, access, and activity instead of relying on periodic reviews.

About Concentric AI

Concentric AI enables organizations to accelerate safe AI adoption through its unified AI and data security governance platform. Powered by the Semantic Intelligence Engine's patented language models, the platform discovers, governs, and protects business-critical and compliance-sensitive data at rest, in motion, and used by AI through a consistent policy framework.

Get a Demo