USE CASE

CONCENTRIC Ai

# Digital Personal Data Protection (DPDP) Compliance

## Your Data Has a New Set of Rules

Data is everywhere. Whether it's a clinic managing medical records, a bank storing financial details, or even an HR department with employee files, companies of all types rely on personal data to operate.

If your organization processes digital personal data in India or serves people in India from elsewhere, you have a set of rules to follow as specified by the Digital Personal Data Protection Act (DPDP Act). The DPDP Act is being phased in, with most obligations taking effect in May 2027, so now is the time to prepare.

Passed in 2023, the DPDP Act defines how your organization collects, uses, shares, and deletes data. If you're handling digital personal data that identifies an individual, you're responsible for protecting it from unauthorized access, misuse, alteration, or destruction. Plus, individuals now have more power to request access, correction, and deletion of their personal data, so your company needs to be ready to respond in a timely manner.

Long story short? If your company deals with digital personal data in India or serves people there, it's time to step up your data protection game.

### The Pain We All Feel

**The data is everywhere.** Personal information is scattered across files, applications, and repositories. Now it may also be shared through AI tools, adding another layer to the visibility challenge.

**Access gets complicated.** Sensitive information may be shared too broadly, exposed through risky permissions, or included in AI prompts and uploads without the right safeguards.

**Compliance isn't a one-and-done.** Data changes, new records appear, and employees find new ways to use information. A point-in-time review can't keep pace with a constantly changing data environment.

### Get Personal Data Under Control

Another privacy regulation doesn't have to mean another mountain of manual work. Understand what personal data you have, identify where stronger protection is needed, and put consistent safeguards in place, including when that data is used by AI.



# Keep Calm and Stay Compliant

When personal data is scattered across cloud, SaaS, and on-premises environments, meeting privacy requirements can become detective work. Concentric AI uses patented language models to understand your data's content and context, helping organizations identify personal information, pinpoint where it resides, and understand how it's exposed.

With a clearer picture of their data, security teams can focus on what needs attention, apply appropriate protections, and respond more efficiently when they need to locate or manage personal data.

- **Know what you're holding.** Identify personal information across structured and unstructured data, including records that traditional pattern-matching approaches may miss.
- **See who has access.** Uncover excessive permissions and risky sharing that could leave personal information exposed to the wrong people.
- **Find the right records.** Locate relevant personal data across your environment to help support access, correction, and deletion requests.
- **Take action where it counts.** Apply classifications, adjust access, and move, copy, or delete data as appropriate to your organization's policies.

## Less Guesswork. Better Data Protection.

Better data intelligence helps your organization:

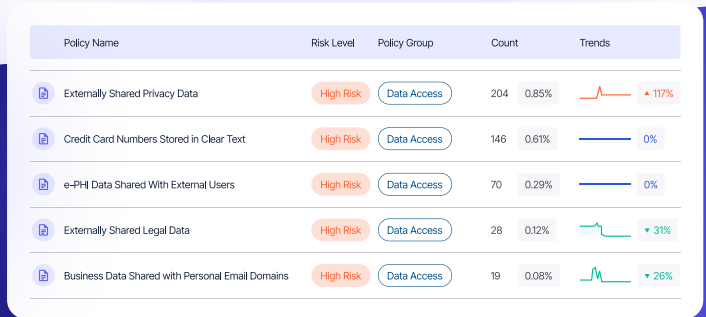
**Get ahead of exposure** by spotting personal information that is overshared or accessible to the wrong people.

**Spend less time searching** when you need to locate personal data across a sprawling data environment.

**Make privacy processes** more manageable with a clearer view of the information your organization holds and how it's accessed.

**Keep pace with changing data** as new records appear, permissions shift, and information moves across your environment.




## 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