

Concentric AI for PDPA Compliance

Sri Lanka has raised the bar on data privacy. The Personal Data Protection Act (PDPA), No. 9 of 2022 made Sri Lanka the first country in South Asia to pass stand-alone data protection legislation, modeled closely on the European Union's General Data Protection Regulation (GDPR). If your organization processes the personal data of customers in Sri Lanka, or offers goods and services there, the PDPA likely applies to you.

The Act gives individuals real rights over their data, including the right to access, correct, and request deletion of their personal information. It also requires organizations to implement operational requirements covering consent, cataloged records of processing, breach notification, and cross-border transfer controls.

The Act was written with AI in mind. Enterprises will need to know what personal data is being fed into their models, copilot, and algorithms. They'll also need to demonstrate a lawful basis for those uses, and show that appropriate safeguards are in place.

The PDPA becomes fully operational on January 1, 2027, which means the runway to get compliant is shrinking—and the penalties are stiff. The Data Protection Authority of Sri Lanka can levy fines of up to LKR 10 million per violation, with penalties escalating for repeat offenses.

Guessing Is Not a Strategy

Many organizations are approaching the 2027 deadline much as they have approached previous new privacy laws: they are not entirely sure where to begin.

Customer personal data is scattered across file shares, email, HR systems, CRM platforms, and increasingly the AI tools their employees use for everyday work.

The Act presupposes something most enterprises lack: an accurate, current picture of what personal data they hold, where it resides, and who can access it.

Without knowing this, PDPA compliance is more guessing than governance. The problem is, guesswork doesn't hold up well under regulatory scrutiny.

The Countdown Has Begun

PDPA enforcement arrives with the new year, but implementing an effective data governance program doesn't happen overnight.

You need a solution that can accurately discover and protect your customers' personal data wherever it is—tucked into cloud folders, buried in old email threads, sitting in on-premises storage, or pasted into an AI prompt.

Build the Evidence Base the PDPA Requires

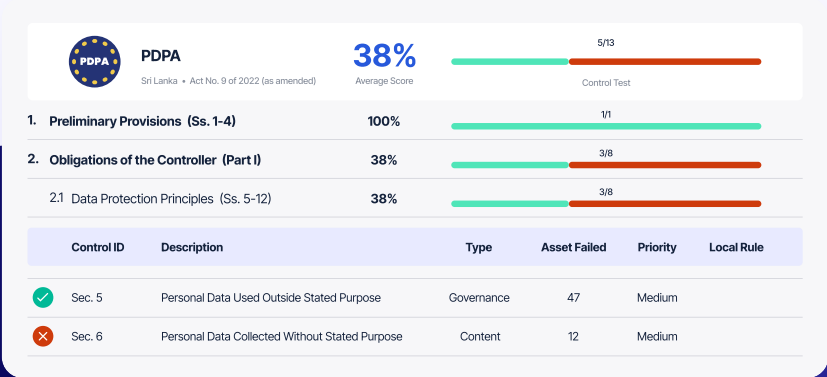
Concentric AI discovers all your data—structured and unstructured, in the cloud and on-premises. No agents, complex rules, or months of manual configuration. Point the solution at your repositories and it gets to work, going beyond rules, regex, patterns, and metadata to deeply understand data in context.

Powered by Concentric AI's Semantic Intelligence™ engine's patented language models, the Concentric AI platform discovers, governs, and protects business-critical and compliance-sensitive data at rest, in motion, and as it is used by AI through a consistent policy framework.

It uncovers PII and other PDPA-regulated personal data with high accuracy, applies classification labels that work with your other security tools, and stops sensitive data from leaking into public AI tools before they become compliance incidents.

The platform continuously monitors for risks such as over-permissioned access, risky external sharing, and unclassified data. When a data subject exercises their right to access or deletion, you can locate every copy of their information without digging through a digital haystack. And you can easily set automated retention policies so data is not kept longer than the PDPA allows.

The Compliance Dashboard, which is already mapping status for GDPR, CCPA, HIPAA, PDPA, and more, easily extends to include other relevant regulatory frameworks.



Visibility, Control, and Compliance

Here's what happens once Concentric AI is watching over your data: the guesswork goes away, and you get answers.

Comprehensive mapping:

Understand exactly where PDPA-regulated personal data exists across your environment, and how it's being accessed and shared.

Accurate classifications:

Protect personal data without restricting legitimate access.

Permission clarity:

Gain full visibility into permissions, including the access nobody remembers granting and nobody should still have.

Automated remediation:

Set policies to identify and stop personal data leakage, without manual intervention.

Audit-ready evidence:

Get proof you can hand straight to the Data Protection Authority, no late-night scrambling required.

About Concentric AI

Concentric AI enables organizations to accelerate safe AI adoption through its unified AI and data security governance platform by protecting data at rest, in motion, and as it is used by AI. Contact us today to schedule a live demo and see for yourself how Concentric AI can help you get PDPA ready.



Schedule a Demo