Digital Personal Data Protection Act of 2023:
Are You Ready?

Since 2017, the right to privacy has been recognized as a fundamental right in India. But what does that mean in the era of digital business?

The Digital Personal Data Protection Act (DPDP) of 2023 attempts to clarify the rights citizens have over their personal information. It also establishes the efforts local and international businesses must make to responsibly manage and protect their customers' personal data.

Unlike other regulatory regimes that govern personal data (such as the General Data Protection Regulation in the European Union), the DPDP does not contain specific provisions for certain types of "sensitive" data.

But the DPDP is new and the implementation schedule still somewhat undefined. Nevertheless, covered businesses will need to make significant effort to prepare–or be at risk of facing regulatory scrutiny and potentially hefty fines. What can you do today to protect your customers' data and prepare for DPDP?

PREPARING YOUR ORGANIZATION

Businesses identified by the DPDP as "data fiduciaries" (that is, persons, companies and government entities who process data) will need to prepare for the implementation of the new law. Here are 3 key efforts that can help you get started.

- **Discover and organize existing personal data:** If you don't know what your exposure is, you can't take steps to remediate. So an essential first step is to take stock of the personal data you currently hold, and understand the data supply chain that carries personal data in and out of your business.

- **Review current data protection policies:** Different industries are already governed by more (or less) restrictive regulatory regimes. By analyzing the policies you already have in place, you can discover the gap between your current data access policies and your business requirements for managing personal data.

- **Prepare for a data breach:** These days, cyberattacks are a near inevitability. And Data/Privacy regulations have evolved to include requirements for protection of personal data, as well as timely reporting in the event of unauthorized access to that data. Penalties can be steep, so preparation is essential.

HOW RUBRIK CAN HELP

Rubrik has helped businesses of all sizes manage requirements for data regulations and privacy laws in various jurisdictions. Rubrik's award-winning offerings provide a robust mechanism for enforcing business objectives to data storage and flow.

This keeps data safe and secure, without compromising production workflows. All work and processes occur on your backup data so your users and production environments remain unaffected.

SENSITIVE DATA DISCOVERY AND CLASSIFICATION

- **Rubrik Sensitive Data Monitoring** is a SaaS application that uses your organization's backup data to discover, classify, and report on sensitive data.

- **Pre-built, customizable policy templates** are available for common categories of personal data.

- **Reports and analytics** on data locations, compliance progress, and policy violations are easily available.

USER ACCESS MONITORING

- Rubrik User Access Analysis proactively identifies which users have access to what data in your organization–allowing you to set appropriate access levels to personal data and **identify data over-exposure.**

- It also identifies and assesses the risk of **over-privileged and unqualified data access,** and identifies which users might pose a security risk.

- **Minimal impact on production environments.**

- **Forensics data for incident response** enables you to quickly identify who had access to the impacted data and identify potentially compromised user credentials.

DATA BREACH PREPARATION

- Rubrik's integration with Zscaler Data Loss Prevention (DLP) proactively identifies sensitive business data across the enterprise so specific protections can be implemented to easily prevent data loss.

- Policies determining the retention and archiving of data can be **mapped to business level SLAs.**

- **Role-based access controls** are available to restrict access and assign user permissions for sensitive data.

- **Data is encrypted both in transit and at rest** for retention policies for on-premise or cloud archival locations.

- **Archived data is encrypted** to prevent unauthorized access.

GET STARTED WITH RUBRIK

Rubrik is a cybersecurity company and our mission is to secure the world's data. We pioneered Zero Trust Data Security to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, built with a Zero Trust design and powered by machine learning, delivers complete cyber resilience in a single platform across enterprise, cloud, and SaaS. Our platform automates data policy management and enforcement, safeguards sensitive data, delivers data threat analytics and response, and orchestrates rapid cyber and operational recovery.

rubrik