



Automate Privacy, Protect Data & Govern AI



Your trusted Partner for DPDPA Compliance

Is your organization equipped to navigate this landscape efficiently?

Implement DPDP Act and Minimize Data Risks with Automated Privacy Solutions

The Digital Personal Data Protection Act (DPDPA) is designed to protect personal data and enhance privacy rights, mandating businesses to manage data responsibly and securely. Implementing DPDPA helps organizations reduce data risks by enforcing stricter controls over data collection, processing, storage, and sharing. Ardent Privacy offers innovative solutions to simplify the complex requirements of DPDPA compliance. With automated tools for data discovery and mapping, organizations can identify where sensitive personal data resides across their systems. Privacy risk assessment features help businesses evaluate vulnerabilities and take corrective action, while centralized dashboards ensure seamless regulatory reporting and real-time monitoring.

Ardent Privacy helps businesses streamline compliance, minimize risks, and build a secure, privacy-conscious ecosystem, fostering trust and safeguarding stakeholder interests in the digital age.

"India's DPDPA introduces penalties of up to ₹250 crore for data breaches, marking a new era of stringent data privacy enforcement."



Financial

GLBA
PCI DSS
FCRA
RBI

Health Care

HIPPA
HITECH

Telecom

GDPR
ECPA

Federal

CMMC
FISMA
Fed RAMP

Security

ISO27001
ISO27701
SOC2

Education

FERPA

Roadmap to DPDPA compliance in 6 steps with TurtleShield

Conduct DPIA and Risk Assessments

Perform Data Protection Impact assessment and Risk Assessments to identify applications and business processes handling PII and to assess compliance

Act - Section 10 | Rule - 13

 Assessment Manager

Discover PII (Personal Data Bill of Materials)

Perform Data discovery, Data Mapping and build Data Bill of Materials (DBoM), Record of Processing activities (RoPA) to understand the data that your organization owns of the Data Principal

Act- Section 8, 10, 11 & 13 | Rules - 6, 7 & 8

 Data Discovery and Intelligence

Implement (DPRM)

> Build secure portal for Data Principal to exercise their rights (submit requests such as Right to access, Right to Erasure and Right to Correct) and privacy teams to manage and fulfill requests
> Enable privacy and data teams to take actions on Data Principal Rights using data discovery module

Act - 8, 11, 12, 13 & 14 | Rules - 14

 Data Principal Rights Management

Implement Data Breach Management and Notification

Automate internal data breach management and internal/external notification process to respond within stipulated timeframes by enabling systems/workflows for notification to the affected Data Principals and to the Data Protection Board and other authorities to meet regulatory requirements without any delay

Act - 8 | Rule - 7

 Data Breach Management

Enforce Storage Limitation Requirements

Establish data retention rules & data deletion schedules as per rules depending on class of data fiduciary (e-commerce, social media and online gaming)

Act - 8 & 12 | Rule - 8

 Data Minimization

Establish Centralised Consent Management system

> Build a centralised system for collecting, verifying, revoking consent, and managing privacy notices and preferences
> Enable verifiable parental/guardian consent (for children/for persons with disabilities) and integrate your consent system with multiple consent managers

Act- 4, 5, 6, 8 & 9 | Rules - 3, 10 & 11

 Unified Consent Management

DPDP Timelines

Intimate each affected Data Principal and Data Protection Board of data breach without any delay

Granular details to the Data Protection Board within 72 hours of being aware of data breach

1. Retain logs and personal data for one year for detection, investigation, remediation of unauthorised access
2. Retain personal data, associated traffic data and logs for one year unless required by other law

Notify Data Principals at least 48 hours prior data erasure giving them time to take action

Data deletion by e-commerce entities and social media companies with not less than 2 cr users in India, or online gaming platforms with not less than 50 lakh registered users within 3 years if the Data Principal hasn't engaged

Maintenance of consent records for 7 years by the Consent Manager

Immediate

72 hours

1 Year

48 hours

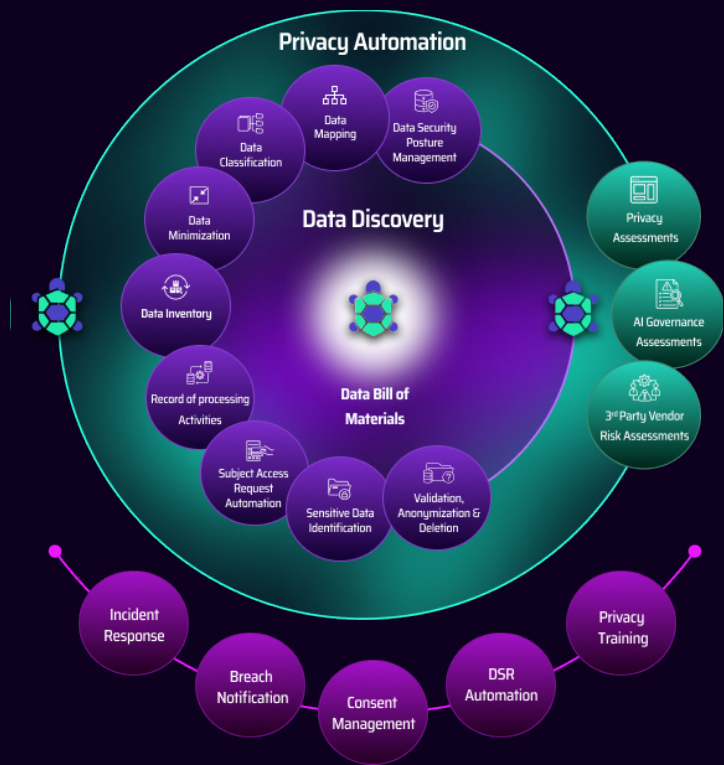
3 Years

7 Years

INTRODUCING TURTLESHIELD

One platform for all your compliance needs

TurtleShield revolutionizes how Data Protection Officers (DPOs) and Chief Information Security Officers (CISOs) manage compliance for Privacy, Security & AI Governance. This robust platform provides an auditable system of record, incorporates a unified control framework, and ensures unwavering compliance while bolstering consumer trust. With TurtleShield, enterprises seamlessly conduct data inventories—including creating comprehensive Data Bills of Materials—perform detailed privacy assessments, and meet all compliance obligations with tools for consent management, training, and breach response. Our unique integration of Privacy Automation with Data Discovery automates tasks, reduces errors, and significantly increases efficiency, freeing up your time to focus on other strategic initiatives. This allows businesses to expand and adapt to more legal frameworks effortlessly and at no additional cost. Start with our pre-built templates for immediate compliance assurance and focus on growing your business securely and confidently with TurtleShield.



TURTLE SHIELD™

Privacy & AI Governance Automation Platform

Common control framework

- | | | |
|---|---|-----------------------------------|
| Assessment Management (DPIA Automation) | Subject Access Requests Fulfillment | AI Governance |
| Incident Response & Breach Notification | Single System of Record | 3rd Party Vendor Risk Assessments |
| Training & Awareness | Unified Consent & Preference Management | Assessment Templates |



Patented Rapid Data Discovery Platform

- | | | |
|-----------------------------------|--------------------------------------|----------------------------------|
| Data Inventory | Data Mapping | Sensitive Data Identification |
| Data Classification | Validation, Anonymization & Deletion | Data Minimization |
| Subject Access Request Automation | Record of Processing Activities | Data Security Posture Management |

Data Bill of Materials (DBOM)

Unblock the power of A.I.

Discover why TurtleShield stands above the rest.

Data-Centric Approach

TurtleShield's data-focused approach leverages its patented Data Discovery solution along with a comprehensive Data Bill of Materials (DBOM), ensuring rapid identification and meticulous management of sensitive personal data.

Deep Domain Expertise

TurtleShield is founded by a team of domain experts whose deep industry expertise ensures comprehensive and practical privacy compliance solutions tailored to dynamic market needs.

Seamless Integration

TurtleShield's seamless integration helps enterprises uphold their privacy standards without disrupting existing workflows. This is enhanced by its low-code common control framework for privacy automation, ensuring continuity and significantly reducing the cost of privacy

Single Source of Truth

TurtleShield offers an auditable system of record (SoR), providing organizations with verifiable evidence of their security and privacy measures, which enhances trust with regulators and customers.

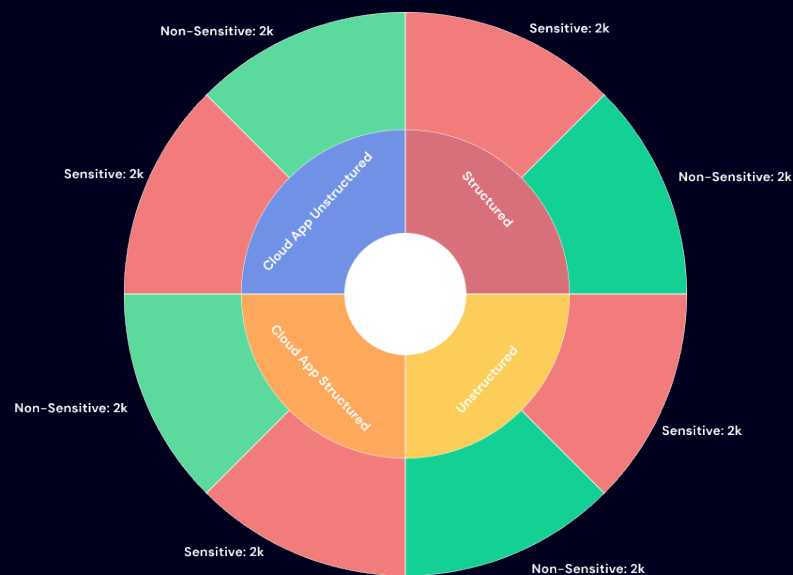


Hear From Our Customers

"We find the Ardent team very collaborative while working on our project. They work with us as an integrated team of bank, very hand in hand, and they are always ready to support us to any extent.."

CISO

India's Largest Pvt Sector Bank



Data Bill of Materials

CONTACT US NOW

+91 [7498281428](tel:7498281428)

advisor@ardentsec.com

[/ardent-privacy](https://www.linkedin.com/company/ardent-privacy)

5520 Research Park Dive
Suite 100, Catonsville, MD,
21228, United States.

Plot #847, SR No. 113/2
Veerbhadr Nagar Road, Baner,
Pune, 411045, India.

4th Floor DSCI, Plot No. 7-10
NASSCOM Campus, Sector
126, Noida, Uttar Pradesh
201303, India.

www.ardentprivacy.ai