DPDP COMPLIANCE PLAYBOOK

Why DPDP Matters for Your Business (Why Start Now)

Progressive

Why organizations must act early

Regulatory accountability is real

DPDP places direct responsibility on the organization (Data Fiduciary), not vendors.

Penalties are material

Non-compliance can lead to significant financial penalties and reputational damage, ₹250 crore for failure to prevent breaches and significant penalties for consent, notice, and rights violations

Customer & employee trust

How you handle personal data directly impacts brand credibility.

Digital growth increases exposure

Cloud, SaaS, AI, and remote work multiply personal data touchpoints.

Compliance takes time

Data discovery, consent redesign, and governance cannot be fixed overnight.

Future readiness

DPDP will influence contracts, audits, and enterprise risk frameworks going forward.

> DPDP is not just a regulation - it is a business risk and trust issue.

Progressive's DPDP Operating Model

28 Years of Trust

PHASE 1: DPDP Readiness & Risk Assessment

What DPDP Needs

DPDP requires the Data Fiduciary to understand:

- What personal data it processes
- Where compliance gaps exist
- What risks may affect individuals' data

What Progressive Techserve Does

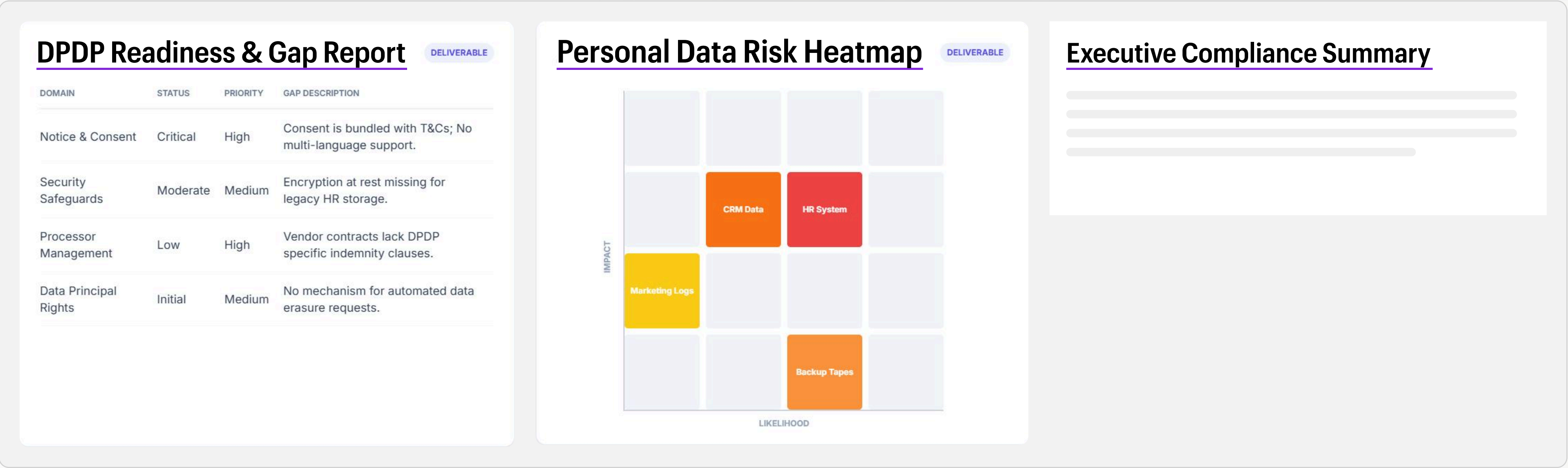
- Identify where personal data exists across business functions
- Assess DPDP applicability and compliance gaps
- Identify high-risk systems, vendors, and processes
- Create a practical remediation roadmap

What the Business Gets

- Clear visibility of DPDP risk exposure
- Prioritized actions instead of legal jargon
- Alignment between IT, security, legal, and business teams

Deliverables

- DPDP Readiness & Gap Assessment Report
- Personal Data Risk Heatmap
- Executive Compliance Summary



DPDP Readiness & Gap Report DELIVERABLE

DOMAIN	STATUS	PRIORITY	GAP DESCRIPTION
Notice & Consent	Critical	High	Consent is bundled with T&Cs; No multi-language support.
Security Safeguards	Moderate	Medium	Encryption at rest missing for legacy HR storage.
Processor Management	Low	High	Vendor contracts lack DPDP specific indemnity clauses.
Data Principal Rights	Initial	Medium	No mechanism for automated data erasure requests.

Personal Data Risk Heatmap DELIVERABLE

Executive Compliance Summary

Early movers reduce cost, risk, and disruption. Late movers face fire drills.

PHASE 2: Personal Data Discovery & Classification

What DPDP Needs

DPDP expects the Data Fiduciary to know what personal data it holds and where it is stored.

What Progressive Techserve Does

- Discover personal data across:
  - Applications (CRM, HRMS, ERP)
  - Cloud storage and file servers
  - Email and collaboration tools
- Classify data by sensitivity and usage
- Map how data flows across systems and vendors

DPDP Compliance Is a Continuous State

DPDP compliance evolves as:

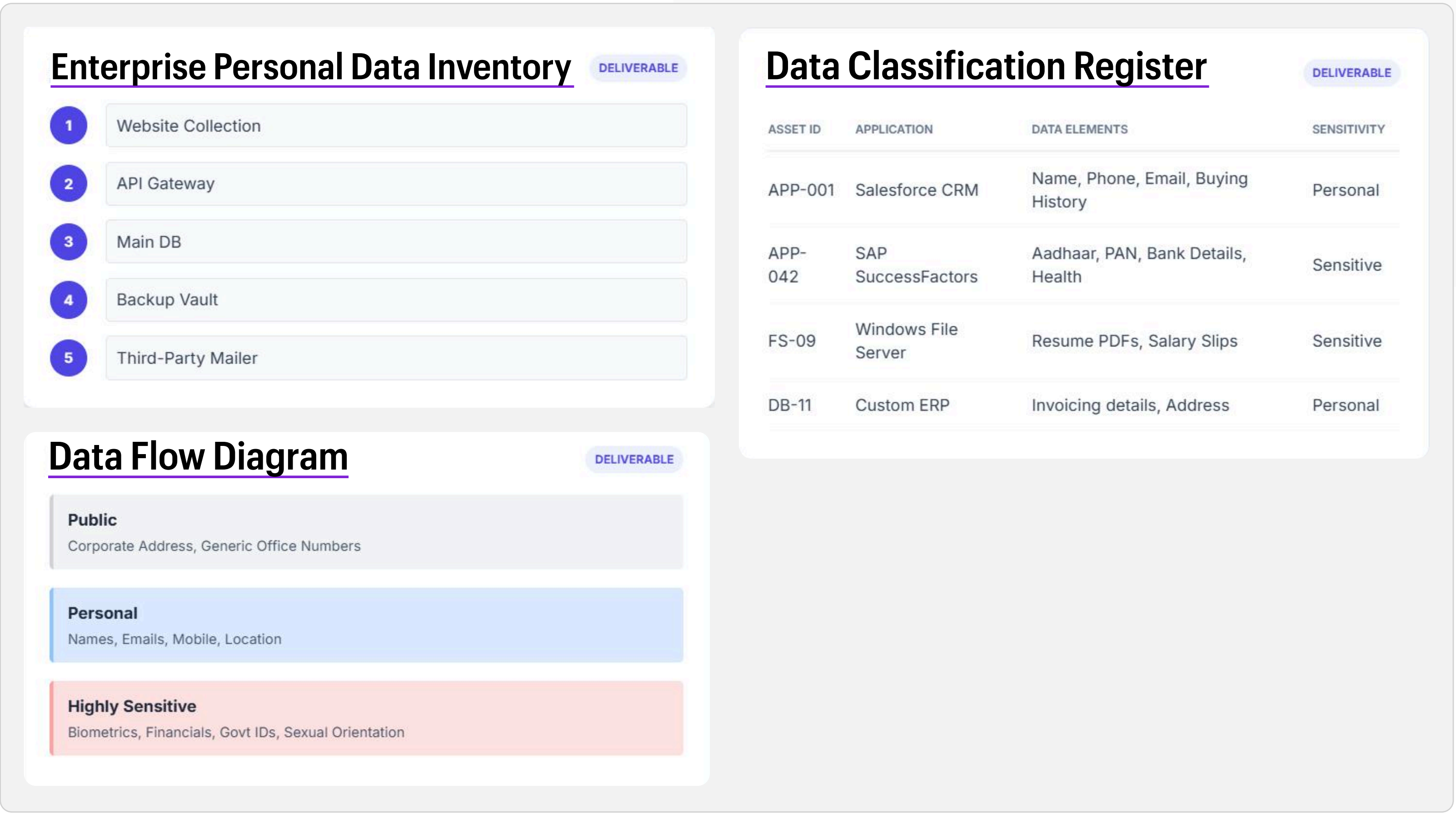
- New applications are introduced
- New vendors are onboarded
- New data is collected
- Business processes change

What the Business Gets

- System-level personal data visibility
- Reduced blind spots during audits or breaches
- Inputs for access control, DLP, and zero-trust initiatives

Deliverables

- Enterprise Personal Data Inventory
- Data Classification Register
- Data Flow Diagrams



Enterprise Personal Data Inventory DELIVERABLE

1. Website Collection
2. API Gateway
3. Main DB
4. Backup Vault
5. Third-Party Mailer

Data Classification Register DELIVERABLE

ASSET ID	APPLICATION	DATA ELEMENTS	SENSITIVITY
APP-001	Salesforce CRM	Name, Phone, Email, Buying History	Personal
APP-042	SAP SuccessFactors	Aadhaar, PAN, Bank Details, Health	Sensitive
FS-09	Windows File Server	Resume PDFs, Salary Slips	Sensitive
DB-11	Custom ERP	Invoicing details, Address	Personal

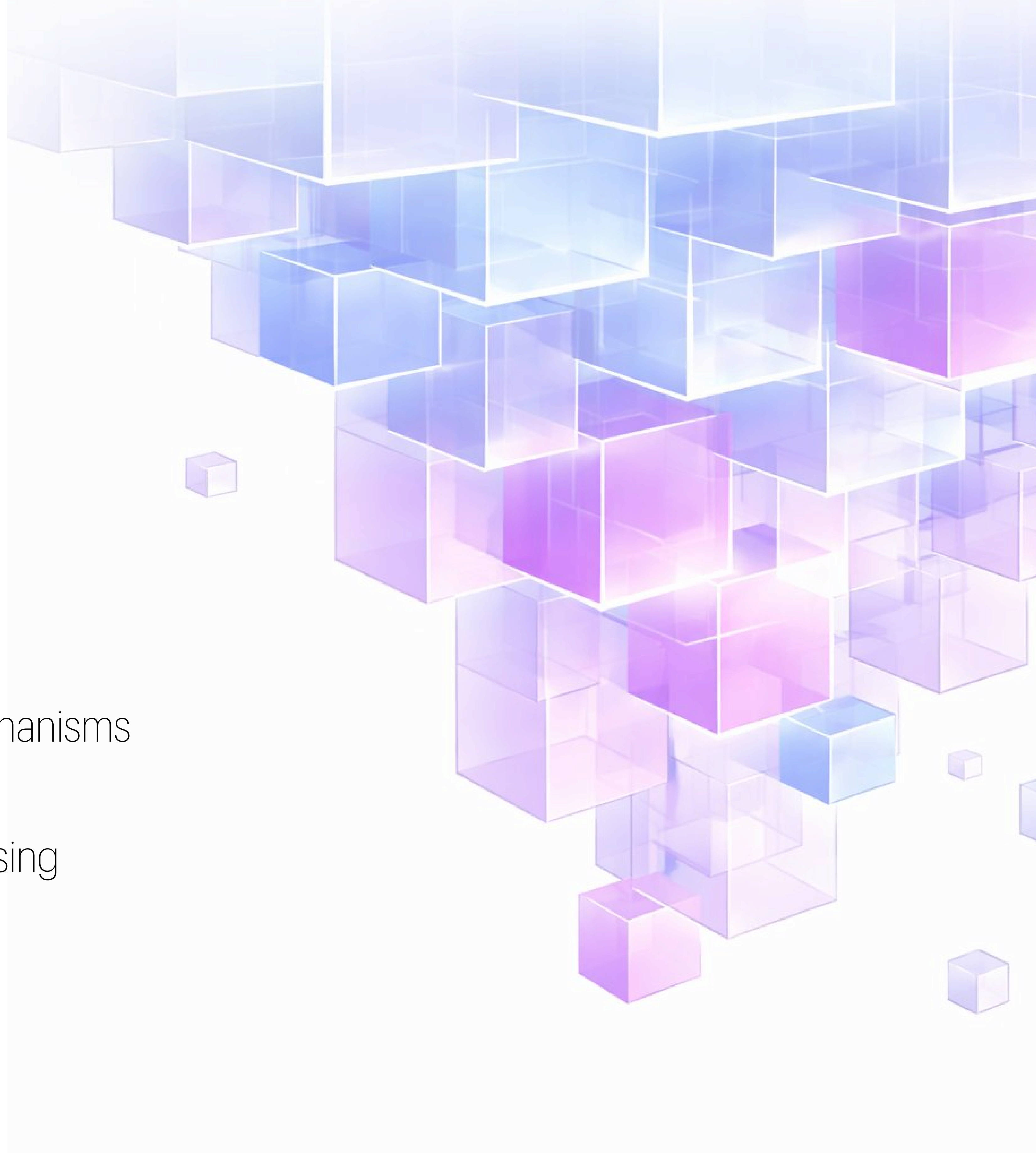
Data Flow Diagram DELIVERABLE

Public
Corporate Address, Generic Office Numbers

Personal
Names, Emails, Mobile, Location

Highly Sensitive
Biometrics, Financials, Govt IDs, Sexual Orientation

> What you don't discover, you can't govern or protect. Unknown data is unmanaged risk.



PHASE 3: Purpose Limitation, Notice & Consent Management

What DPDP Needs

DPDP requires that personal data is:

- Collected for a clear, lawful purpose
- Explained to the Data Principal through a notice
- Processed only after valid consent (where required)

What Progressive Techserve Does

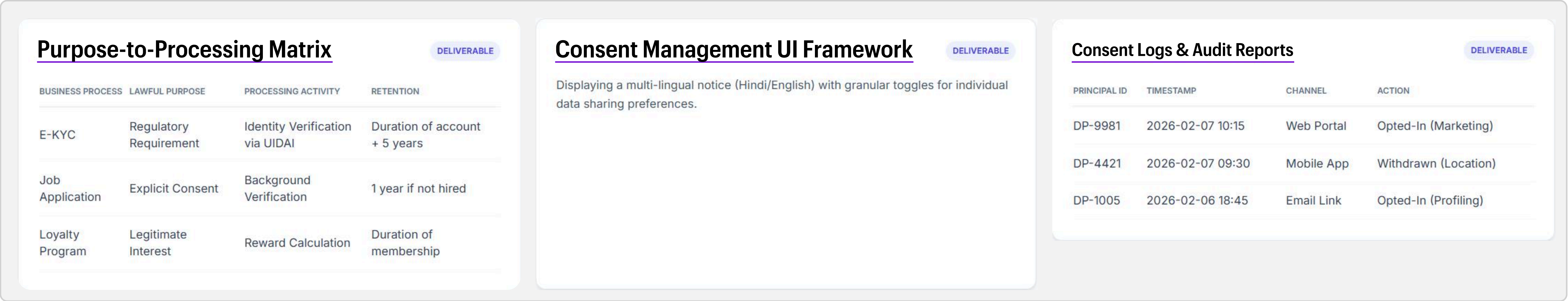
- Map data usage to business purposes
- Design consent capture and withdrawal mechanisms
- Implement consent logging and traceability
- Align privacy notices with actual data processing

What the Business Gets

- Defensible consent records
- Reduced legal and regulatory exposure
- Transparent data usage governance

Deliverables

- Purpose-to-Processing Matrix
- Consent Management Framework
- Consent Logs & Audit Reports



Purpose-to-Processing Matrix DELIVERABLE

BUSINESS PROCESS	LAWFUL PURPOSE	PROCESSING ACTIVITY	RETENTION
E-KYC	Regulatory Requirement	Identity Verification via UIDAI	Duration of account + 5 years
Job Application	Explicit Consent	Background Verification	1 year if not hired
Loyalty Program	Legitimate Interest	Reward Calculation	Duration of membership

Consent Management UI Framework DELIVERABLE

Displaying a multi-lingual notice (Hindi/English) with granular toggles for individual data sharing preferences.

Consent Logs & Audit Reports DELIVERABLE

PRINCIPAL ID	TIMESTAMP	CHANNEL	ACTION
DP-9981	2026-02-07 10:15	Web Portal	Opted-In (Marketing)
DP-4421	2026-02-07 09:30	Mobile App	Withdrawn (Location)
DP-1005	2026-02-06 18:45	Email Link	Opted-In (Profiling)

Purpose defines legitimacy under DPDP. Data without purpose or consent creates exposure.

PHASE 4: Data Principal Rights & Governance Workflows

What DPDP Needs

DPDP gives the Data Principal (individual) the right to:

- Access their data
- Correct inaccuracies
- Request deletion
- Raise grievances

The Data Fiduciary must respond within defined timelines.

What Progressive Techserve Does

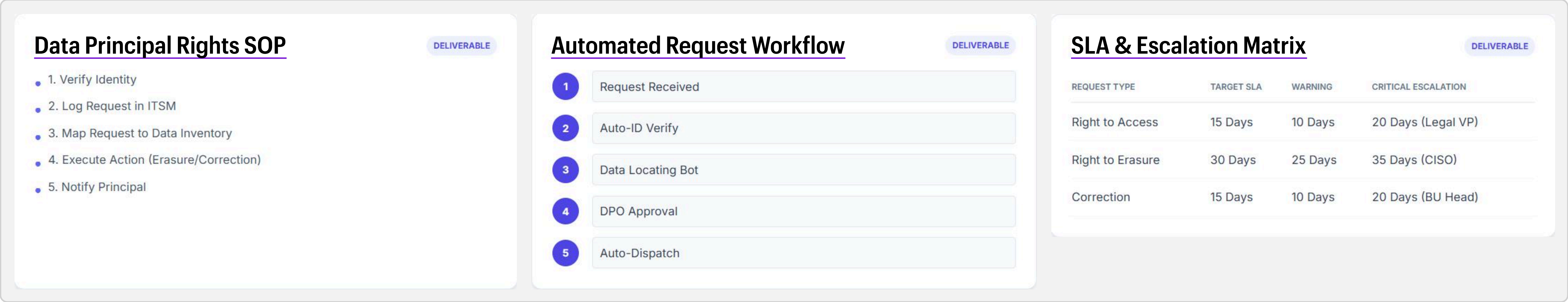
- Design workflows to handle these requests
- Integrate with ITSM / service desk tools
- Define ownership, SLAs, and escalation paths

What the Business Gets

- Structured, auditable request handling
- Reduced operational chaos
- Clear cross-functional accountability

Deliverables

- Data Principal Rights SOPs
- Automated / Semi-Automated Request Workflows
- SLA & Escalation Matrix



Data Principal Rights SOP DELIVERABLE

- 1. Verify Identity
- 2. Log Request in ITSM
- 3. Map Request to Data Inventory
- 4. Execute Action (Erasure/Correction)
- 5. Notify Principal

Automated Request Workflow DELIVERABLE

1. Request Received
2. Auto-ID Verify
3. Data Locating Bot
4. DPO Approval
5. Auto-Dispatch

SLA & Escalation Matrix DELIVERABLE

REQUEST TYPE	TARGET SLA	WARNING	CRITICAL ESCALATION
Right to Access	15 Days	10 Days	20 Days (Legal VP)
Right to Erasure	30 Days	25 Days	35 Days (CISO)
Correction	15 Days	10 Days	20 Days (BU Head)

Rights must be operational, not theoretical. Delayed responses invite scrutiny.

PHASE 5: Security Safeguards & Breach Readiness

What DPDP Needs

DPDP requires reasonable security safeguards to protect personal data and readiness to manage breaches.

What Progressive Techserve Does

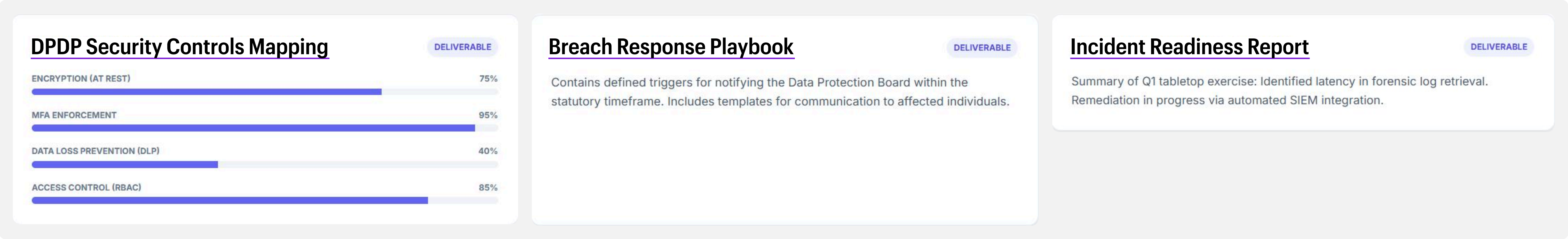
- Align existing security controls to DPDP requirements
- Strengthen access controls, encryption, and monitoring
- Create breach response playbooks specific to personal data
- Conduct breach readiness simulations (optional)

What the Business Gets

- DPDP-aligned security posture
- Faster breach response
- Reduced regulatory and reputational impact

Deliverables

- DPDP Security Controls Mapping
- Breach Response Playbook
- Incident Readiness Report



DPDP Security Controls Mapping DELIVERABLE

ENCRYPTION (AT REST) 75%

MFA ENFORCEMENT 95%

DATA LOSS PREVENTION (DLP) 40%

ACCESS CONTROL (RBAC) 85%

Breach Response Playbook DELIVERABLE

Contains defined triggers for notifying the Data Protection Board within the statutory timeframe. Includes templates for communication to affected individuals.

Incident Readiness Report DELIVERABLE

Summary of Q1 tabletop exercise: Identified latency in forensic log retrieval. Remediation in progress via automated SIEM integration.

Controls reduce incidents. Readiness limits damage when breaches occur.

PHASE 6: Vendor & Third-Party Data Governance

What DPDP Needs

When personal data is shared with Data Processors DPDP requires:

- Contractual safeguards
- Ongoing oversight

What Progressive Techserve Does

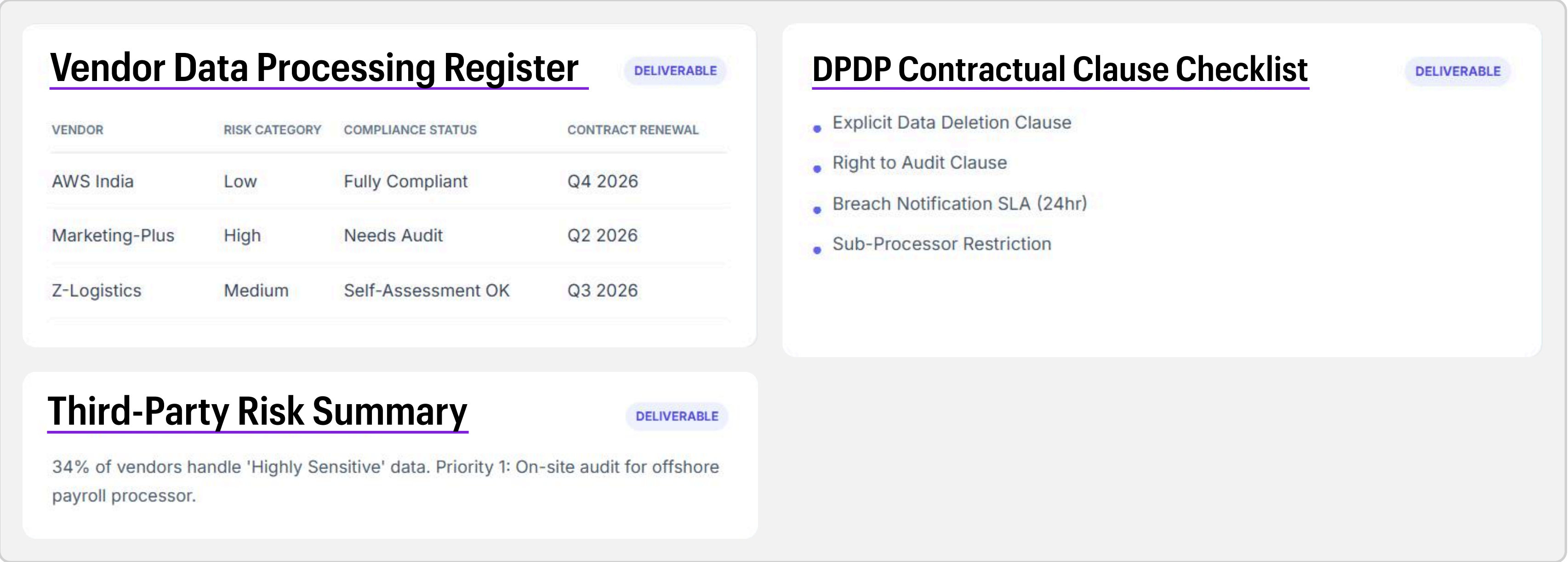
- Identify vendors handling personal data
- Review contracts for DPDP-aligned clauses
- Classify vendors based on data risk
- Establish vendor compliance checks

What the Business Gets

- Reduced third-party data risk
- Clear processor accountability
- Improved audit readiness

Deliverables

- Vendor Data Processing Register
- DPDP Contractual Clause Checklist
- Third-Party Risk Summary



Vendor Data Processing Register DELIVERABLE

VENDOR	RISK CATEGORY	COMPLIANCE STATUS	CONTRACT RENEWAL
AWS India	Low	Fully Compliant	Q4 2026
Marketing-Plus	High	Needs Audit	Q2 2026
Z-Logistics	Medium	Self-Assessment OK	Q3 2026

DPDP Contractual Clause Checklist DELIVERABLE

- Explicit Data Deletion Clause
- Right to Audit Clause
- Breach Notification SLA (24hr)
- Sub-Processor Restriction

Third-Party Risk Summary DELIVERABLE

34% of vendors handle 'Highly Sensitive' data. Priority 1: On-site audit for offshore payroll processor.

> Data sharing does not transfer accountability. Vendor failures become fiduciary risk.

PHASE 7: Continuous DPDP Compliance (Managed Services)

What DPDP Needs

DPDP is not one-time compliance must be continuous as systems and data change.

What Progressive Techserve Does

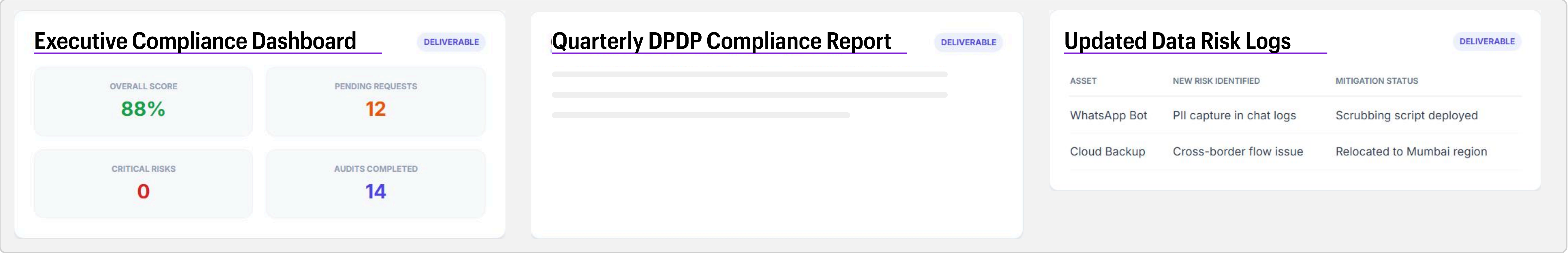
- Monitor new systems, data flows, and vendors
- Update data inventories and risk registers
- Provide periodic compliance reports
- Track regulatory updates

What the Business Gets

- Predictable compliance operations
- Reduced internal workload
- Always audit-ready posture

Deliverables

- Quarterly DPDP Compliance Reports
- Updated Data Inventories & Risk Logs
- Executive Compliance Dashboard



Executive Compliance Dashboard DELIVERABLE

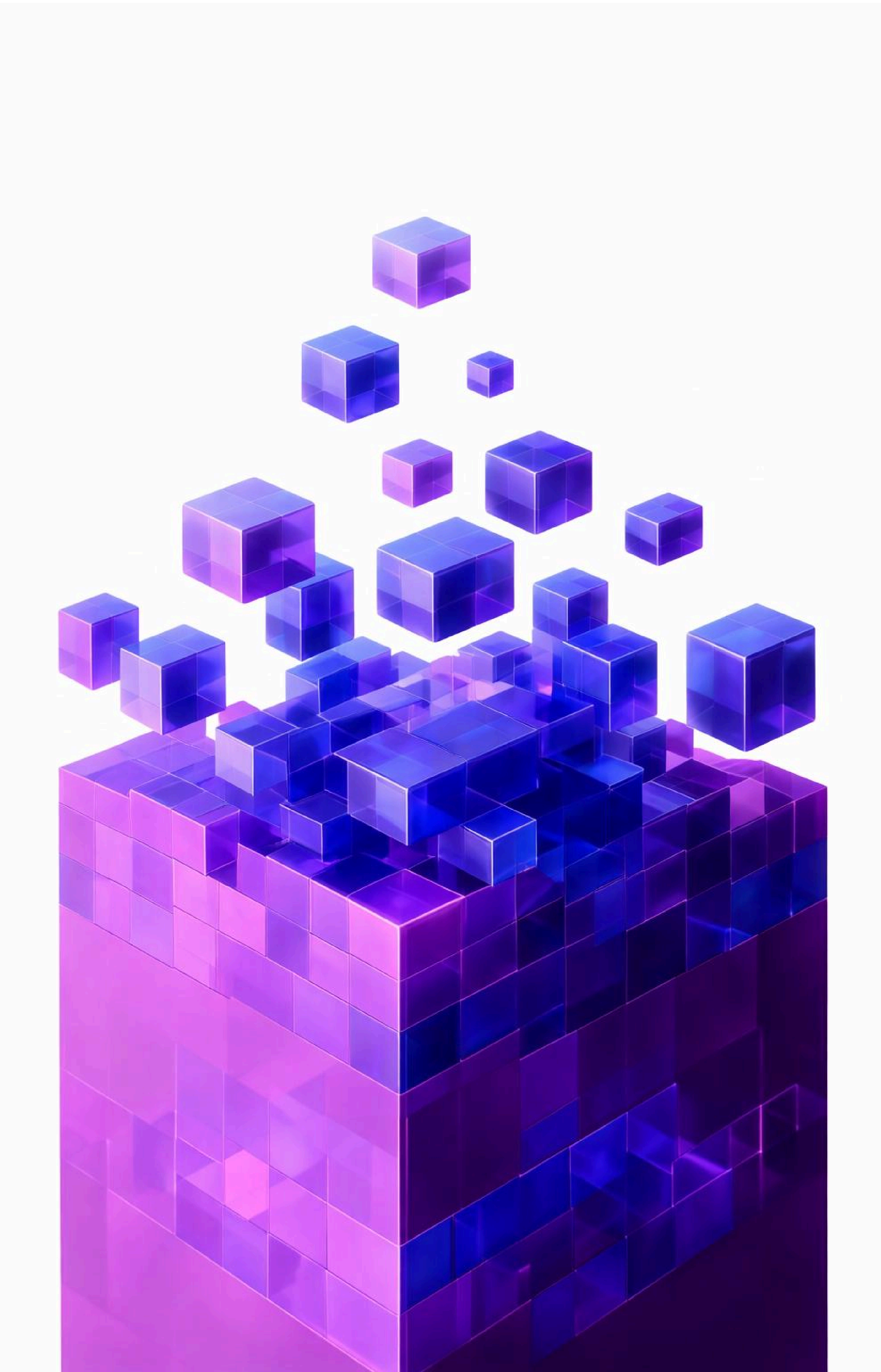
OVERALL SCORE	PENDING REQUESTS
88%	12
CRITICAL RISKS	AUDITS COMPLETED
0	14

Quarterly DPDP Compliance Report DELIVERABLE

Updated Data Risk Logs DELIVERABLE

ASSET	NEW RISK IDENTIFIED	MITIGATION STATUS
WhatsApp Bot	PII capture in chat logs	Scrubbing script deployed
Cloud Backup	Cross-border flow issue	Relocated to Mumbai region

DPDP compliance is not static. Continuous oversight prevents compliance decay.



If We Do All This... Are We DPDP Compliant?

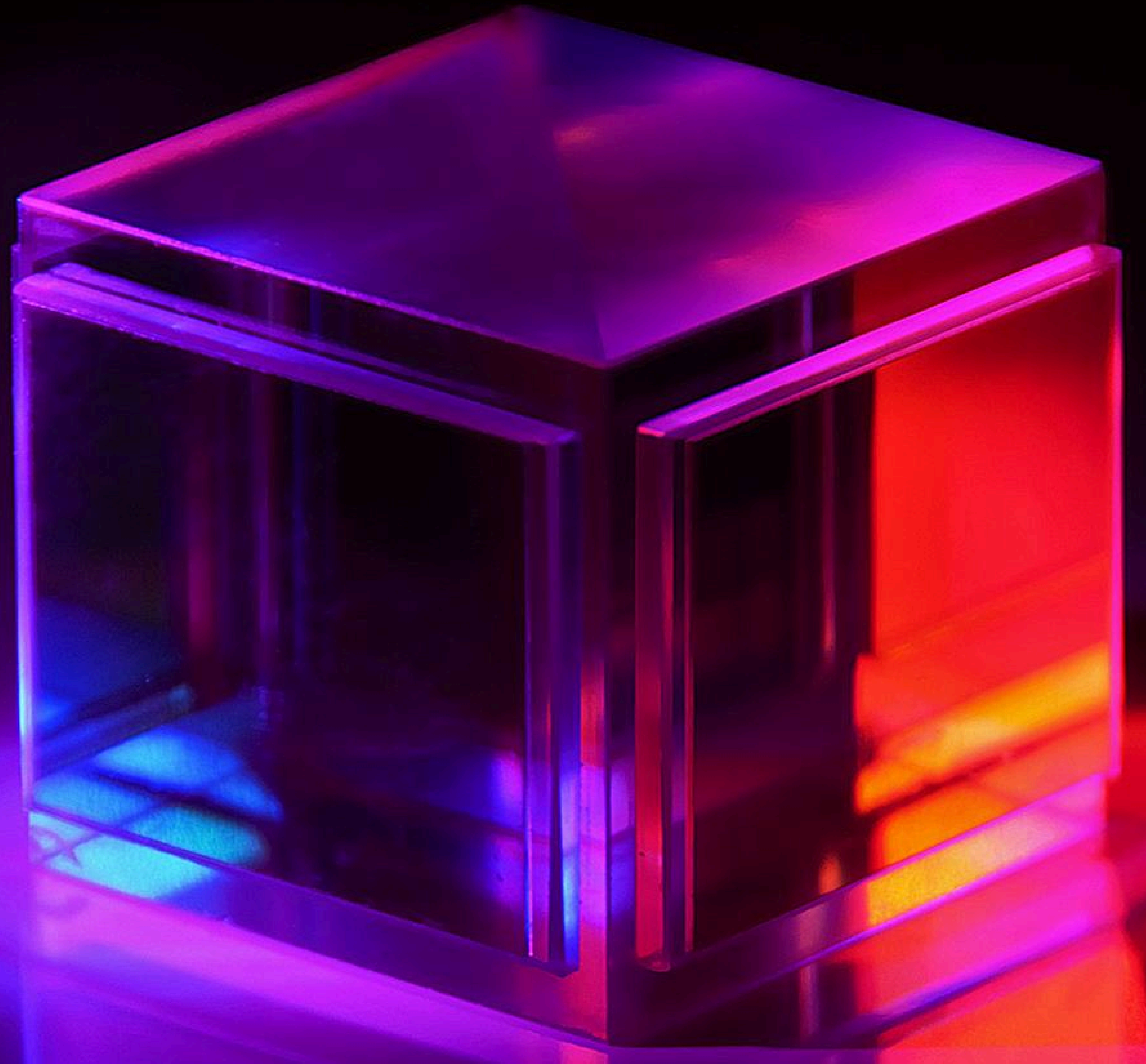
You become DPDP-aligned and operationally compliant.

DPDP compliance is not a one-time certificate. It is a state of readiness and accountability.

By completing all phases in this playbook, you achieve:

- ✓ Clear ownership of personal data
- ✓ Lawful and transparent data usage
- ✓ Ability to respond to Data Principal requests
- ✓ Reasonable security safeguards
- ✓ Breach response readiness
- ✓ Documented evidence of compliance

This is what regulators expect in practice.



*DPDP compliance is about protecting people's data and your organization's trust.
Progressive Techserve ensures this is done clearly, securely, and continuously - without burdening your teams.*

How Progressive Ensures You Stay Compliant

Progressive Techserve does not “close a project and walk away”.

We:

- Monitor compliance posture continuously
- Update controls as your environment changes
- Maintain audit-ready documentation
- Act as your extended DPDP office

✉ solutions@progressive.in

🌐 www.progressive.in

Our role is to keep you compliant while you focus on running the business.