FAQs on DPDPA & CERT-In

Toolkit for the Aug 7, 2025 Masterclass

Prepared by	Elytra Security
Date	August 7, 2025
Document Classification	Public

DPDPA & Cybersecurity Masterclass – FAQs and Expert Answers

GENERAL COMPLIANCE FAQs

Is DPDPA applicable even if we're already compliant with ISO 27001 or GDPR?
A: Yes. ISO 27001 and GDPR provide a strong baseline, but DPDPA is India-specific. It introduces obligations such as local consent language, grievance handling mechanisms, notice formats, and engagement with the Data Protection Board.

Do all companies need a Data Protection Officer (DPO) or Consent Manager?
A: Only *Significant Data Fiduciaries* (as designated by the government) are formally required to appoint a DPO. However, any business collecting personal data should assign someone responsible for privacy to ensure readiness and accountability.

How can small and midsize firms comply if they don't have privacy or security teams?
A: Lean documentation, a readiness checklist, and a simple RACI chart for responsibilities can go a long way. DPDPA is about demonstrable accountability — not headcount. Focus on intent, clarity, and action.

What are the absolute essentials to show you're DPDPA-ready?
A: At minimum:

- Privacy Policy
- Consent Capture Records
- Grievance Redressal Mechanism
- Notice Templates
- Incident Response Plan
- Retention Guidelines
- Basic RoPA (Record of Processing Activities)

What are the fines, and who is at highest risk?
A: Penalties can go up to ₹250 crore per violation. High-risk sectors include financial services, healthcare, EdTech, and any business handling children's data, biometrics, or large data volumes — especially if they lack breach readiness.

Can we reuse our global privacy policy for India?
A: No. DPDPA requires simplification, localization, clarity on lawful purposes, and explicit consent management — especially in Indian languages. Templates made for GDPR often miss these nuances.

CERT-In & INCIDENT RESPONSE FAQs

What kinds of incidents must be reported to CERT-In?
A: Ransomware, data breaches, unauthorized access, attacks on critical systems, and even certain phishing or DDoS events — especially if you're in a regulated sector (SEBI, RBI, IRDAI, etc.).

What's the current reporting window for CERT-In?
A: Within **6 hours** of detection for covered entities. This includes submitting the full incident report and sharing logs upon request. Early containment and escalation processes must be built in advance.

Do non-regulated companies need to worry about CERT-In?
A: While mandatory for certain sectors, being CERT-In ready is quickly becoming a corporate governance norm. Major enterprises, SaaS companies, and B2B vendors are all adopting the standard to build trust and avoid scrutiny.

What exactly needs to be submitted during CERT-In reporting?
A: Details of the incident, detection method, affected systems, remediation actions taken, potential impact, timeline, and contact details. CERT-In templates are available on their website.

What if we don't have 180 days of log data?
A: That's a compliance issue. CERT-In mandates 180-day log retention. You'll need centralized logging (SIEM/EDR/Fluent Bit etc.), preferably with backup and offline storage to meet this requirement.

Who inside the company should lead CERT-In compliance?
A: It's a joint task:

- CISO for technical diagnosis
- DPO or privacy officer for regulatory context
- Legal for report vetting
- Executive sponsor for escalations

A defined **RACI matrix** will help streamline this.

SECURITY & GOVERNANCE FAQs

What does "security by design" mean in practice?

A: It means security is not bolted on — it's embedded. This includes identity controls, secure development, access reviews, vulnerability patching, and breach drills. Compliance without security is a paper tiger.

Who is accountable for breach readiness — CISO or DPO?

A: Both. The CISO owns breach prevention and technical security. The DPO ensures compliance, notification, and redressal. They must work in tandem, especially in incident response situations.

What controls are absolutely essential under DPDPA?

A: Core controls include:

- Encryption of data at rest and in transit
- Role-based access control
- Logging and alerting
- Secure deletion
- Endpoint protection
- Breach response documentation

How often should we perform security audits or VAPT?

A: At least **annually**, or after major infrastructure or code changes. Regulated entities may need to do it **quarterly or bi-annually**. Document your audit history for regulators.

Can vendors or cloud providers be held responsible for data loss?

A: Yes — but only if your contracts enforce it. Legally, the *Data Fiduciary* (you) are always accountable. That's why Data Processing Agreements (DPAs) and vendor controls are critical.

How do we start building a security culture internally?

A:

- Set the tone from the top
- Train staff quarterly
- Conduct mock breaches or tabletop exercises
- Publish security tips internally
- Create incentive mechanisms for good behavior

VENDOR RISK & CONTRACTS FAQs

What kinds of vendor contracts must be updated for DPDPA?

A: Any vendor handling personal data on your behalf must sign a DPA (Data Processing Agreement) that covers processing scope, breach notification, sub-processing, and audit rights.

Do SaaS providers need to be audited now?

A: Yes. You must ask vendors about their breach history, security controls, CERT-In compliance, and DPDPA readiness. High-risk vendors should be assessed annually and documented in your **Vendor Risk Register**.

What do we do if a critical vendor refuses to sign a DPA?

A: Raise it with leadership. You may need to negotiate tighter terms, switch providers, or mitigate through compensating controls (e.g., anonymization, firewalling, local backups). But don't proceed blind.

Are cloud providers like AWS and Azure DPDPA-compliant?

A: They offer compliant tools, but compliance depends on your usage. You must configure roles, access policies, regions, and retention settings carefully — and document everything.

Should we map all our vendors in a single sheet or tool?

A: Yes. Maintain a **Vendor Inventory Tracker** showing:

- Name
- Data type handled
- Risk rating
- Contract status
- Last assessment date
  This shows due diligence if questioned.

DPDPA Understanding & Readiness

What are the top 3 practical actions companies should take to prepare for DPDPA today?

A: Here are the 3 most practical actions you can do today

- Run a Privacy Gap Assessment against DPDPA to identify missing elements (consent, notice, data rights, breach response).
- Create or update a Privacy Policy with Indian law–specific language.
- Establish a Record of Processing Activities (RoPA) to document data flows and lawful basis for processing.

Does DPDPA apply to employee data or just customer data?

A: Yes, it applies to **both**. Employee data is personal data. Employers are required to issue notices, justify processing under lawful basis (e.g., employment contract), and protect employee data rights.

How should we handle older data collected before DPDPA came into effect?

A: You need to either **revalidate consent** (if consent was not DPDPA-compliant), or **assign a lawful basis** for retention. If neither is possible, the data should be anonymized or deleted.

What's the real-world difference between a 'Data Principal' and a 'Data Fiduciary'?

A:

- **Data Principal**: The individual whose personal data is being collected.
- **Data Fiduciary**: The organization deciding the purpose and means of processing that data.

Think: **Employee = Principal; HR Dept = Fiduciary.**

Is DPDPA enforcement already active, or are we in a transition phase?

A: We're in a **pre-enforcement phase**, but regulators have signaled urgency. Smart organizations are acting now to reduce liability and build trust.

What are the actual penalties under DPDPA, and who bears the liability in practice?

A: Penalties go up to ₹250 crore. **Organizations bear primary liability**. However, **directors and officers** may be held accountable under related laws (e.g., IT Act, Companies Act) if negligence is proven.

Do small companies (under 100 employees) need to comply fully with DPDPA?

A: Yes. There are **no exemptions based on size**. Every company processing personal data is subject to DPDPA. Smaller entities can adopt **simplified toolkits** to demonstrate intent and accountability.

Is DPDPA applicable even if we're already compliant with ISO 27001 or GDPR?

A: Yes. ISO 27001 is a *security* standard. GDPR is *extraterritorial* but tailored for the EU. **DPDPA is Indian law**, with specific roles (e.g., Data Principal, Grievance Officer), timelines, and procedural expectations. You must **map controls** from ISO/GDPR to DPDPA, but DPDPA compliance still requires **distinct documentation and readiness.**

What happens if we don't appoint a DPO or Consent Manager immediately?

A: Not all companies are required to appoint a DPO **by default**. However, if your organization is notified as a **Significant Data Fiduciary (SDF)** — based on volume, sensitivity, or risk of data processing — you **must** appoint a DPO. Even if you're not formally notified, it is **strongly recommended** to designate someone as a **privacy lead or DPO-equivalent**, especially in sectors like finance, healthcare, IT, or education, where sensitive data is regularly handled. This role should report to the Board or a senior authority. **Pro tip**: Use an internal owner or outsource to services like **Elytra vDPO** temporarily.

How do small businesses practically demonstrate compliance without full-time teams?

A: Simple solutions exist

- Use prebuilt templates and checklists (like Elytra's Starter Toolkit)
- Maintain a RoPA, simple risk register, and documented privacy policy
- Assign internal roles (e.g., HR = Consent Manager)

- Train employees with short privacy modules
- Record everything — evidence matters more than perfection

What is the minimum set of documentation needed to defend a DPDPA compliance claim?

A: At a minimum:

- RoPA
- Risk Register
- Consent Records
- Privacy Notices
- Incident Response SOP
- Grievance Redressal Register
- Training Logs
- Evidence of policy communication

Even basic, Excel/Word versions are valid if they're **structured, updated, and accessible**.

What are the penalties under DPDPA and who is most at risk?

A: Penalties range up to **₹250 crore per violation**.

High-risk entities:

- Data-rich startups collecting sensitive personal data
- HRTech, FinTech, HealthTech, EdTechs with minors' data
- Companies with poor breach response or no grievance redressal

Directors can be held liable if governance lapses are proven.

How should we update privacy policies in light of DPDPA — just a banner or more?

A: A **banner is not enough**. You must:

- Use layered notices (summary + detailed)
- Clearly explain purpose, retention, data sharing
- Allow withdrawal and correction
- Update policies every time processing changes

Can we use a global privacy policy template for India?

A: Only if it's **localized**. You must:

- Replace terms like "Data Subject" with "Data Principal"
- Reference DPDPA rights and Grievance Officer details
- Include specific India-related practices, retention, and contact points.

Otherwise, it may be considered **non-compliant or misleading.**

What kind of documentation will a DPDPA auditor or regulator expect to see?

A: At a minimum, all of these

- Privacy Policy & Notice
- Consent Logs
- RoPA (Record of Processing)
- Risk Register
- Data Subject Rights log
- Breach Reporting SOP
- Training records

Do we need consent for everything? Are there any lawful grounds for processing without consent?

A: No, **consent is not always required**. DPDPA allows **legitimate uses** such as employment, legal obligations, or public interest. But **transparency and notices** are still mandatory.

CERT-In Breach Reporting and Incident Response

Which industries are currently bound by CERT-In 6-hour breach reporting?
A: All **entities in India**—regardless of sector—must report certain cyber incidents to CERT-In within **6 hours** of detection. This includes IT service providers, cloud companies, financial institutions, health, telecom, and any business using IT infrastructure.

What happens if we miss the 6-hour CERT-In deadline?
A: Failure to comply can lead to **investigations, fines, and reputational damage**. Repeat violations can attract legal action under the IT Act. Even unintentional delays must be documented with justification.

Can breach reports to CERT-In be sent by email, or is there a formal process?
A: Reports must be submitted using the **CERT-In Incident Reporting Format** and emailed to **incident@cert-in.org.in**. Large entities may need to integrate with CERT-In's portal for structured submissions.

Is internal fraud or insider theft considered a "cyber incident" under CERT-In?
A: Yes. If it involves **unauthorized access, data theft, or misuse of systems**, it falls under CERT-In's mandate—even if it's an insider. The broader interpretation includes employee-based breaches.

How do we manage breach notification if we're using outsourced IT or a cloud provider?
A: You remain the **primary responsible party**. Vendor contracts should mandate prompt breach disclosure to you, so **you can meet your reporting obligations** within 6 hours.

Who should be the single point of contact with CERT-In from our organization?
A: Ideally, the **CISO or an incident response lead**. CERT-In requires organizations to designate a **formal Point of Contact (PoC)** via their registration form and keep that info up to date.

What systems and logs do CERT-In expect us to maintain — and for how long?
A: CERT-In mandates **log retention for 180 days** for specified events. This includes:

- Firewall and system logs
- VPN and user authentication logs
- Application access logs
- Endpoint detection logs
  Logs should be stored in India and made available on demand.

Does CERT-In allow a grace period for investigation before reporting publicly?
A: Yes. CERT-In requires **prompt reporting to them**, but **public disclosure is not immediate**. You can complete internal investigations before going public, unless legally required to disclose earlier.

Operational Integration: Privacy + Security + Risk

How do we embed DPDPA controls without overwhelming our teams?
A: Start with a phased approach using clear ownership. Use a **RACI matrix** to define who's Responsible, Accountable, Consulted, and Informed. Focus first on **notice, consent, data mapping, and breach response**. Break implementation into weekly or biweekly sprints—just like tech delivery. Avoid one-off workshops and instead focus on **ongoing integration into existing processes** (e.g., onboarding, vendor reviews, access control).

What's the best way to structure the privacy-security collaboration operationally?
A: Establish a **Privacy-Security Governance Cell** or joint working group. Define clear hand-offs:

- Security handles technical safeguards (access, encryption, firewalls, logs)
- Privacy handles data rights, consent, lawful basis, and breach notification
  Use **shared dashboards**, conduct **joint tabletop exercises**, and **align on risk scoring** so neither side duplicates effort.

We already have ISO 27001 — how much more is DPDPA work beyond that?
A: ISO 27001 covers **security of information**, not **lawful processing of personal data**. DPDPA adds:

- Consent and notice obligations
- Data Subject Rights (access, erasure, correction)
- Grievance redressal
- Lawful basis for processing
- Data principal communications

You can leverage ISO 27001 controls, but **additional legal, HR, and customer-facing processes** are needed.

What KPIs or metrics should we track for privacy program maturity?
A: Key metrics include:

- % of systems with updated privacy notices
- % of employees trained on DPDPA
- Number of subject rights requests handled and resolved on time
- Time to respond to incidents
- % of vendors with signed DPAs (Data Processing Agreements)
- Audit scores for policy implementation and data handling

Should the CISO or Legal own privacy implementation in India?
A: Neither alone. DPDPA is a **cross-functional mandate**. Ideally:

- Legal owns interpretation and external-facing legal obligations
- IT/CISO owns infrastructure and technical controls
- Privacy Lead coordinates implementation, training, and audits

In small companies, this may be the same person—but the **accountability must be shared.**

How do we convince the business side (sales, HR, marketing) to support DPDPA efforts?
A: Tie privacy to **business risk and trust**:

- Sales: Avoid penalties that could disrupt contracts or credibility
- HR: Employee data is covered—noncompliance could cause labor disputes
- Marketing: Privacy-friendly messaging improves brand trust

Showcase **regulatory penalties**, customer expectations, and **loss of business** due to poor privacy practices.

How do we tie in DPDPA with our existing vendor contracts and SLAs?
A: Update your vendor contracts with:

- Data Processing Addendums (DPAs)

- Specific breach notification timelines
- Obligations to assist with audits, subject rights, and compliance
- Defined liability clauses

  Use a Vendor Risk Assessment template and tag vendors by risk category (e.g., high-risk = payroll, IT, cloud). Review these annually.

Risk Registers, SOPs, and Documentation

What's the difference between a risk register and a RoPA (Record of Processing Activities)?
A: A **Risk Register** documents *threats, vulnerabilities, and potential impact* to personal data—e.g., "HR laptop theft may lead to data leak." A **RoPA** catalogs *where and how personal data is processed*—e.g., "Payroll data stored in XYZ cloud service, retained for 8 years."

RoPA tells what exists. Risk Register tells what could go wrong.

How do we assign risk scores in the DPDPA context?
A: Use a **3x3 or 5x5 matrix**:

- Likelihood (Rare, Possible, Likely)
- Impact (Low, Medium, High)

Multiply both to get a **risk score**, then assign:

- Mitigation owner
- Control
- Review date

Example: "WhatsApp data sharing" = Likely × High = Critical Risk → Mitigate or stop

Can you give examples of high-risk processing under DPDPA for Indian companies?
A: Common high-risk cases:

- Processing biometric or health data (e.g., facial recognition in attendance)
- Cross-border data transfers without DPA safeguards
- Surveillance or tracking of employees without purpose limitation
- Sharing customer data with third parties (e.g., insurance aggregators)
- Processing children's data (under 18)

How frequently should risk registers and SOPs be updated?
A:

- Risk Registers: Quarterly or when a major system/vendor/process changes
- SOPs: Annually or when regulations/processes change
- After every breach or major incident, both should be reviewed and updated.

Is it okay to use Excel and Word documents for DPDPA tracking, or do we need a tool?
A: Yes, **Excel and Word are fine** to start with—especially for small and mid-sized firms.
But use version control, restrict editing, and **back them up**.
Upgrade to tools (like ElytraGRC or OneTrust, TrustArc, etc.) when scale demands **automation, access control, and audit trails**.

What templates should we start with if we have no privacy team today?
A: Begin with these:

- Privacy Policy (external + internal)
- RoPA (Record of Processing Activities)
- Risk Register
- Consent Log
- Incident Response SOP
- Grievance Redressal SOP
- Staff Training Tracker

These can be **simple, fillable formats**, not over-engineered.

Do we need to maintain audit logs of policy acceptance and employee training?

A: Yes. Under DPDPA, you must demonstrate:

- Staff were *aware of their obligations*
- Policies were *communicated and acknowledged*
- Trainings were *conducted and tracked*

Use email records, LMS logs, or acknowledgment forms—**digital or paper-based—but traceable**.