Technology Update

Cyber Security and Privacy in Governance

Integrating Cyber Security and Data Protection under the DPDP Act, 2023

Edited by **MOHAN DAS VISWAM**

When a hospital's digital systems freeze under a ransomware attack or a citizen's Aadhaar-linked data leaks online, the damage extends far beyond lost files — it erodes public trust. Each such incident reminds us that cybersecurity without privacy is incomplete, and privacy without cybersecurity is impossible.

The Digital Personal Data Protection (DPDP) Act, 2023 marks a watershed moment in the nation's digital governance journey. For the first time, citizens have enforceable rights over their personal data, and organizations are bound by clear obligations to protect it. Yet, passing a law is only the beginning. The true challenge lies in translating the Act's intent into daily governance — ensuring that personal data is not only processed lawfully but also shielded from breaches, misuse, and negligence.

This is where Cyber Information Security Governance becomes indispensable. By creating structured accountability across people, processes, and technology, it turns legal compliance into operational discipline. A well-governed cybersecurity framework ensures that data protection is not a reaction to a breach but a culture embedded into every digital system.

In essence, the DPDP Act provides the legal backbone, but cyber governance provides the muscle and memory to make it work. Together, they lay the foundation for a privacy-first, cyber-resilient, and citizen-trust-driven Digital India.

C.J. Antony
Dy. Director General & HoG
antony@nic.in

Manoj K. Kulshreshth
Sr. Technical Director
mkk@nic.in

The Digital Personal Data Protection (DPDP) Act, 2023 establishes citizens' rights over personal data and mandates organizations to ensure its protection. However, true compliance requires Cyber Information Security Governance — a framework that embeds accountability, vigilance, and discipline across systems, people, and processes. By uniting privacy and cybersecurity under one governance model, organizations can move from reactive compliance to proactive trust-building. Sector-specific models, unified oversight, and a culture of accountability are essential to operationalize the Act. Ultimately, cyber governance transforms data protection from a legal requirement into a culture of digital responsibility, resilience, and citizen trust.

Why Cyber Governance Matters After DPDP

The Digital Personal Data Protection (DPDP) Act, 2023 mandates that every organization adopt "reasonable security safeguards" to protect personal data. But in the complex digital ecosystem of government systems, start-ups, and public platforms, what exactly counts as reasonable? Technology alone cannot answer that question. It requires structure, accountability, and foresight — the very essence of Cyber Information Security Governance.

Cyber governance provides the framework that transforms compliance into consistency. It ensures that protecting personal data is not left to individual judgment or afterthought but becomes part of an institution's design. Instead of reacting to threats, governance creates a proactive system of checks and balances that continuously monitors, evaluates, and improves security posture.

At its core, Cyber Governance bridges law and technology through discipline. It aligns cybersecurity controls with DPDP's privacy principles — from data minimization and purpose limitation to breach notification and consent management. The result is an ecosystem where every department, vendor, and digital platform operates under a unified accountability model.

Key dimensions of Cyber Information Security Governance include:

- **Systemic discipline:** Establishing clear policies, defined roles, and documented procedures to replace ad-hoc or reactive security practices.
- **Risk prioritization:** Safeguarding sensitive categories of data first — such as health, financial, or biometric information — through classification and layered protection.
- **Continuous vigilance:** Recognizing that breaches are inevitable but damage is preventable when detection, response, and reporting systems are well-governed.
- **Integrated compliance:** Embedding cyber safeguards directly into DPDP obligations — such as ensuring informed consent, minimizing data collection, and timely breach disclosures.

In short, cyber governance provides the operating system for DPDP compliance. It gives institutions the capacity to act responsibly, respond swiftly, and recover confidently — turning the principle of "reasonable security" into measurable, auditable, and enduring trust.

Real-Life Examples

Laws express intention; governance tests ex-

ecution. Across sectors, several real-world incidents have shown how fragile systems become when cybersecurity and privacy frameworks operate in isolation — and how resilient they are when governance binds them together.

Take the AIIMS ransomware attack in 2022. A sophisticated intrusion crippled the hospital's servers for weeks, threatening the confidentiality of millions of patient records. The absence of patch management, network segmentation, and timely response amplified the crisis. Under the DPDP regime, such an incident would trigger mandatory breach notifications to both the Data Protection Board and affected citizens — a scenario that underscores the urgent need for structured incident governance, offline backups, and defined escalation channels.

Similarly, the CoWIN data exposure (2021–22) revealed the dangers of weak API governance. Personal details like names, contact numbers, and vaccination status were accessible through unauthorized interfaces. The lesson is clear: API security and third-party oversight must become core governance practices, not technical afterthoughts. Under DPDP, unauthorized disclosure of personal data would constitute a breach of fiduciary duty, inviting accountability and redressal claims.

In contrast, DigiLocker stands as a positive example of governance by design. By encrypting stored documents, minimizing data collection, and empowering citizens to control sharing, it has already operationalized several DPDP principles — including purpose limitation, data minimization, and user consent. It proves that privacy-first architecture is achievable when governance leads design, not when it follows regulation.

Global experiences also offer valuable cues. In 2023, Meta was fined €1.2 billion under the GDPR for transferring user data to the United States without adequate safeguards. This case is a stark reminder that cross-border data governance is not a procedural formality — it's a cornerstone of trust. For Indian organizations expanding globally, compliance with DPDP's cross-border transfer provisions will demand similar rigor.

Each of these examples converges on one principle: Cyber Governance turns compliance into culture. Where governance was weak, breaches turned into crises; where governance was strong, trust became the default.

Sector-Specific Governance Models for Cyber & Data Protection

No two sectors face identical risks. A hospital's responsibility toward patient records differs fundamentally from a bank's obligation to secure financial transactions or a telecom operator's duty to protect subscriber identity.

▼ Tab 11.1 **Real-Life Examples**

Case	Governance Lesson	DPDP Relevance / Key Takeaway
AIIMS Ransomware Attack (2022)	Weak patching and delayed response crippled hospital systems.	Mandatory breach reporting to DPB; highlights need network segmentation, offline backups, and incident governance.
CoWIN Data Exposure (2021-22)	Insufficient API governance led to unauthorized data access.	Unauthorized disclosure breaches fiduciary duty; emphasizes strong API security and third-party audits.
DigiLocker Platform	Encryption, minimal data collection, and citizen-controlled sharing ensure privacy by design.	Model example of DPDP principles - consent, purpose limitation, and data minimization in action.
Meta GDPR Fine (2023)	Poor cross-border safeguards in data transfers.	Indian entities must enforce lawful transfer controls under DPDP to avoid similar penalties.

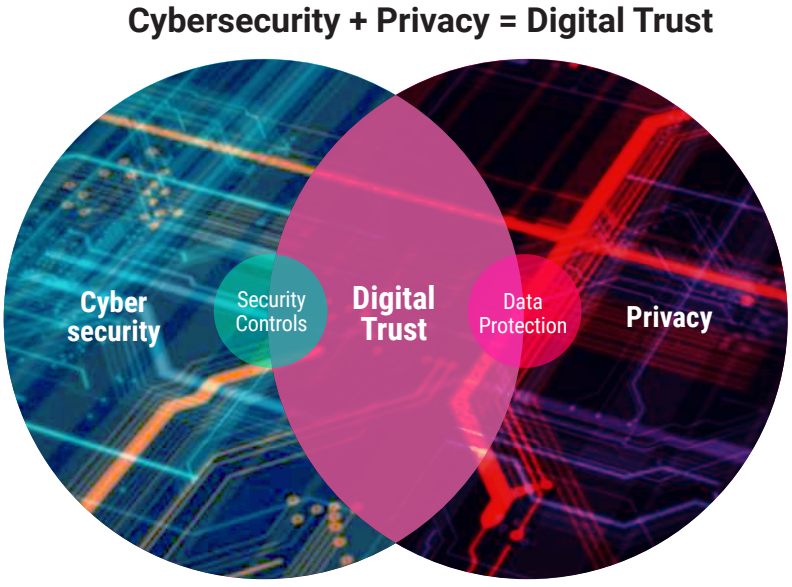
The DPDP Act acknowledges this diversity by demanding context-specific safeguards — a principle that lies at the heart of cyber governance.

In the healthcare sector, ransomware and identity theft remain the biggest threats. Hospitals and telemedicine providers must classify health information as sensitive personal data, encrypt patient records, and conduct regular Privacy Impact Assessments (PIAs). The AIIMS incident showed that without network segmentation and disciplined patching, even critical public institutions can face prolonged disruption.

The financial sector operates under dual regulatory oversight from the RBI and now DPDP. Here, governance translates into adopting Zero Trust Architectures, enforcing multi-factor authentication, and conducting periodic stress tests. The Cosmos Bank cyber heist in 2018 exposed how unmonitored endpoints and weak vendor oversight can compromise even well-regulated entities.

In telecom and digital communications, the focus must shift to data minimization and vendor governance. Telecom operators handle enormous volumes of personal data — from call logs to geolocation trails — making lawful interception policies and cross-border data safeguards indispensable. International cases, like Vodafone UK's GDPR fine, illustrate the risks of weak internal controls and insufficient transparency.

The public sector and e-governance platforms sit at the center of citizen trust. Platforms such as Aadhaar, CoWIN, and DigiLocker demonstrate both the vulnerabilities and strengths of large-



▼ Tab 11.2 **Sector-Specific Governance Models for Cyber & Data Protection**

Sector	Key Risks	Governance Priority	Example / Lesson
Healthcare	Ransomware, identity theft, unauthorized research use	Encrypt health data, restrict access, classify as sensitive, conduct Privacy Impact Assessments	AIIMS ransomware attack - need for segmented networks and timely breach response
Financial Services	Fraud, phishing, insider misuse	Adopt Zero Trust Architecture, enforce multi-factor authentication, align with RBI & DPDP norms	Cosmos Bank heist - endpoint monitoring and strong vendor oversight essential
Telecom & Digital Communications	SIM swap, data misuse, surveillance	Strengthen vendor governance, apply data minimization, ensure lawful interception compliance	Vodafone UK GDPR fine - transparent governance for subscriber data
E-Governance / Public Sector	API leaks, large-scale data exposure	Integrate privacy-by-design, centralize oversight, ensure CERT-In reporting	CoWIN exposure vs. DigiLocker's encryption - contrasting outcomes of governance maturity
Education	Child data exploitation, profiling, identity theft	Secure learning platforms, parental consent for minors, strict EdTech vendor audits	Edmodo breach - need to safeguard DIKSHA and SWAYAM user data
Critical Infrastructure	Ransomware, sabotage, national disruption	Segregate IT/OT networks, adopt NCIIPC frameworks, run red-team drills	Colonial Pipeline attack - highlight for India's smart grid resilience
AI & Emerging Tech Startups	Re-identification, bias, unconsented data use	Implement privacy-preserving AI, ensure consented datasets, maintain audit trails	AI model misuse cases - need for ethical AI governance aligned with DPDP

scale data systems. Integrating privacy-by-design, ensuring CERT-In reporting, and building centralized governance boards are now imperative for all government data systems.

In education, safeguarding student data — particularly of minors — demands parental consent frameworks, secure Learning Management Systems (LMS), and stringent vendor oversight in EdTech collaborations. The Edmodo breach, which exposed millions of student records, highlights why India's DIKSHA and SWAYAM platforms must evolve stronger governance layers.

For critical infrastructure, the risks are existential. Power grids, transport networks, and smart city systems rely on a blend of IT and operational technology (OT). Governance here means strict network segregation, real-time monitoring, and red-team drills aligned with NCIIPC frameworks. The Colonial Pipeline attack in the U.S. serves as a warning: a single breach can disrupt an entire national supply chain.

Finally, AI and emerging technology startups introduce new governance frontiers. Training datasets, behavioral analytics, and generative models raise novel privacy challenges — from re-identification risks to algorithmic bias. DPDP compliance for these entities will hinge on privacy-preserving AI techniques, transparent model governance, and explicit consent for data use in training systems.

Across all sectors, one truth endures: governance must adapt, but accountability remains absolute.

A privacy-aware governance model doesn't just protect systems — it reinforces the social contract between citizens and the institutions that serve them.

Key Governance Areas in the Post-DPDP Era

The Digital Personal Data Protection (DPDP) Act, 2023 is not merely a piece of legislation — it is a transformative milestone that reshapes how organizations in our nation govern, process, and protect personal data. It marks a decisive shift from compliance-based data handling to accountability-driven governance, where protecting citizens' data becomes both a strategic necessity and an ethical obligation.

In this new era, cybersecurity is no longer viewed as a purely technical or IT concern. It has evolved into a board-level priority, requiring active participation from compliance teams, senior management, and business leadership. The Act compels organizations to create structures that blend legal awareness, technological resilience, and organizational culture.

To operationalize this shift, modern governance must focus on six interlinked areas. Together, these form the foundation of a privacy-first and cyber-resilient organization — one that treats data not as a commodity, but as a shared national asset entrusted to its care.

Unified Governance Frameworks

In a world where data flows seamlessly across systems, vendors, and borders, fragmented controls no longer work. Organizations need a single, unified governance framework that integrates privacy and cybersecurity under one model.

Mapping data assets, defining ownership, and aligning policies across departments ensures shared accountability between the CISO and DPO. Unified encryption standards, centralized monitoring, and integrated reporting replace isolated practices, helping organizations move from compliance to true data stewardship.

Breach Response and Reporting

Under the DPDP Act and CERT-In directives,

breaches must be reported swiftly — both to regulators and affected citizens. A strong breach response system requires clear escalation paths, forensic readiness, and transparent communication.

Integrating incident response with privacy obligations helps detect and contain threats while maintaining public trust. In a digital democracy, how fast and how honestly an organization responds to a breach defines its credibility.

Vendor and Third-Party Oversight

Most modern breaches occur through vendors or supply chains. The DPDP Act holds Data Fiduciaries responsible for their partners' lapses, making vendor governance a non-negotiable priority.

Strong oversight includes due diligence before onboarding, embedding compliance clauses in contracts, conducting regular audits, and monitoring vendors continuously. Turning vendors into trust partners rather than risk factors strengthens institutional resilience.

Data Lifecycle Governance

Data protection does not end at collection — it must extend across the entire lifecycle, from creation to deletion. Clear retention schedules, encryption during use, and automated deletion after expiry bring the principle of data minimization to life.

Such lifecycle governance ensures organizations retain only what they need, process only what is lawful, and dispose of data responsibly — converting policy into everyday discipline.

CISO–DPO Collaboration

The post-DPDP era demands close collaboration between cybersecurity and privacy functions. The CISO safeguards how data is protected; the DPO defines why it is collected and for how long.

Joint reviews, shared audits, and coordinated risk assessments help unify security and compliance goals. Together, they build a coherent accountability framework that balances protection with purpose.

Culture of Accountability

Technology can secure systems, but only culture secures organizations. Regular awareness sessions, phishing drills, and password hygiene campaigns turn employees into frontline defenders.

When every team — from vendors to citizen-facing units — treats data as a shared responsibility, governance evolves from compliance to culture.

In essence, these six pillars form the scaffolding of trustworthy digital governance. They remind us that data protection is not a one-time compliance task but a living practice — one that transforms privacy from a legal mandate into a national value, anchoring a resilient and trusted Digital India.

Challenges

Translating the Digital Personal Data Protection (DPDP) Act, 2023 from policy to practice is less about drafting new rules and more about changing how institutions behave. While the law provides direction, implementation faces several operational and cultural hurdles that must be addressed for cyber governance to truly take root.

Defining "Reasonable Safeguards"

The Act's requirement for "reasonable security safeguards" provides flexibility, but also ambiguity. Without concrete benchmarks, interpretations may vary drastically — some organizations may underinvest in protection, while others may overspend on unnecessary controls.

To bring consistency, organizations should anchor their governance in global standards such as ISO 27001 (Information Security), ISO 27701 (Privacy Information Management), or NIST Cybersecurity Framework. When aligned with CERT-In directives, these standards turn "reasonable" into measurable, auditable, and enforceable safeguards.

Balancing Cost and Compliance

For smaller organizations, compliance can feel like an expensive proposition. Implementing encryption systems, conducting audits, or hiring data officers involves real financial and human costs.

A phased compliance model provides a practical pathway — prioritizing high-risk data and critical operations first. The government can play a vital role through shared security infrastructures, compliance toolkits, and capacity-building programs that make privacy protection inclusive and achievable for all organizations, not just the well-resourced ones.

Bridging the Skills Gap

India's data governance ecosystem faces a dual shortage — of cybersecurity experts who understand law, and of lawyers who understand technology. This skills gap hampers consistent compliance maturity across sectors.

To overcome this, NIC, MeitY, and NCIIPC should lead sustained efforts in capacity building, creating specialized training modules for CISOs, DPOs, and government officers. Public-private partnerships with universities and certification bodies can further ensure a steady pipeline of skilled professionals capable of operationalizing the DPDP Act across industries.

Managing Regulatory Overlap

Many sectors already comply with multiple data protection regimes — from the IT Act and CERT-In directives to RBI, IRDAI, and SEBI guidelines. The addition of DPDP risks creating regulatory confusion or "compliance fatigue."

The solution lies in harmonized governance frameworks that treat all these obligations as complementary rather than competing. By mapping overlaps, organizations can streamline reporting, unify audits, and establish a single accountability structure that aligns all regulatory expectations coherently.

Navigating Early Enforcement

DPDP's implementation will evolve as the Data Protection Board issues its first rulings. Until then, compliance expectations may remain fluid.

The best strategy is proactive documentation — recording governance actions, risk assessments, and breach responses — to demonstrate due diligence even amid regulatory uncertainty.

Cyber governance after DPDP is a journey, not a checklist. The challenges are real, but each one offers an opportunity — to set clearer standards, strengthen institutional capacity, and embed accountability deep within digital systems. The law defines the mandate; governance gives it life.

Way Forward

To truly translate the intent of the Digital Personal Data Protection (DPDP) Act, 2023 into public trust, organizations must weave privacy and cybersecurity into their governance DNA. Compliance should not be seen as a checklist but as a mindset guiding every decision. This transformation begins with unified governance—where CIOs, CISOs, and DPOs work together to align technology, policy, and accountability. Regular privacy and security impact assessments, supported by hybrid frameworks like ISO 27001 and 27701, can help manage risks and unify technical and privacy standards. AI-driven monitoring should ensure continuous vigilance, while privacy-by-design principles make protection an integral part of system development. Close collaboration with NIC, CERT-In, and sectoral regulators will further harmonize compliance and strengthen institutional trust.

Ultimately, the post-DPDP era is not about mere legal conformity but about building citizen confidence. Cybersecurity and privacy must evolve from regulatory burdens into a culture of digital responsibility. A truly digital nation is not defined by how many devices it connects, but by the security, dignity, and trust it offers to every connected citizen.

Contact for more details

C.J. Antony
Deputy Director General & HoG
Cyber & Information Security Governance Division
NIC HQ, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: antony@nic.in, Phone: 011-24305740