B5

Data Protection, Cybersecurity & IT Compliance

DPDPA 2023, CERT-In Directions, IT Act Provisions, Cross-Border Data Flows & Sectoral Obligations

BHATT & JOSHI ASSOCIATES — INDIAN ELECTRONICS SECTOR LEGAL SERIES

Data Protection, Cybersecurity & IT Compliance

DPDPA 2023, CERT-In Directions, IT Act Provisions, Cross-Border Data Flows & Sectoral Obligations

Booklet V of VI — Indian Electronics Sector Legal Series

Bhatt & Joshi Associates, Advocates & Legal Consultants

TABLE OF CONTENTS

Chapter 1 — Digital Personal Data Protection Act 2023 3

Chapter 2 — CERT-In Directions 2022 and Cybersecurity Obligations 10

Chapter 3 — IT Act 2000: Electronics Sector Obligations 16

Chapter 4 — Cross-Border Data Flows and Localisation 22

Chapter 5 — Sectoral Obligations: IoT, Smart Products and OEM Compliance 27

CHAPTER ONE

Digital Personal Data Protection Act 2023

Legislative Framework, Data Fiduciaries, Consent Architecture, Data Principals' Rights, and the Data Protection Board

> *The Digital Personal Data Protection Act, 2023 (DPDPA) is India's landmark data protection legislation, establishing a comprehensive framework for the processing of personal data. For electronics companies — from consumer device OEMs to enterprise hardware manufacturers, e-commerce platforms, and embedded software developers — the DPDPA creates significant compliance obligations and strategic commercial considerations.*

1.1 DPDPA: Legislative History and Structure

The Digital Personal Data Protection Act, 2023, enacted by Parliament in August 2023 and receiving Presidential assent on 11 August 2023, replaces the earlier personal data protection bill process that had generated multiple draft bills (the Personal Data Protection Bill, 2019 and its 2021 revision, both of which were withdrawn before enactment) spanning four years of legislative deliberation. The DPDPA represents a significantly simplified architecture compared to its predecessors — dropping the GDPR-inspired provisions on sensitive personal data categorisation, data localisation mandates, and the Data Protection Authority's rate-setting powers in favour of a more technology-neutral, principles-based framework. The Act applies to

the processing of "digital personal data" — data about individuals that is in digital form, or that is collected in non-digital form but subsequently digitised — by "Data Fiduciaries" (entities that determine the purpose and means of processing personal data) and their "Data Processors" (entities that process data on behalf of the Fiduciary). The territorial scope of the Act covers: processing of personal data within the territory of India; and processing of personal data outside India if the processing relates to the offering of goods or services to Data Principals (individuals) within India — the "targeting" criterion that brings international electronics and technology companies within the Act's scope even if they have no physical presence in India. The DPDPA is the primary data governance law for electronics companies whose products collect, process, or transmit personal data of Indian users — a category that encompasses virtually every connected device, smart product, and digital service in the Indian market.

The DPDPA establishes specific obligations for "Significant Data Fiduciaries" (SDFs) — Data Fiduciaries that the Central Government designates as significant based on volume of personal data processed, sensitivity, risk to national sovereignty, or impact on competition and innovation. SDFs are subject to additional obligations not applicable to ordinary Data Fiduciaries: mandatory appointment of a Data Protection Officer (DPO) resident in India; appointment of an independent data auditor to conduct periodic audits; mandatory data protection impact assessments for new processing activities; and restrictions on the transfer of certain categories of personal data to specific countries. For major electronics companies — global smartphone OEMs with millions of Indian device users, large cloud services providers with significant Indian customer bases, and social media platforms embedded in consumer electronics — SDF designation is both likely and commercially significant, as the additional SDF obligations increase compliance costs and restrict data processing flexibility.

1.2 Consent Framework and Deemed Consent

The DPDPA's consent framework requires Data Fiduciaries to obtain "free, specific, informed, unconditional and unambiguous" consent from the Data Principal before processing their personal data, with consent to be signified through a "clear affirmative action" — an active, affirmative indication of agreement rather than passive acceptance or inferred consent from continued use of a service. The Act specifies that consent must be accompanied by a "notice" that is clear and plain (without legalese), available in multiple languages (at least the scheduled languages of India that the Data Principal may request), and that specifically communicates the purpose of data collection, the categories of personal data to be collected, and the rights of the Data Principal. For electronics OEMs whose products collect personal data through embedded sensors, cameras, microphones, location services, and usage analytics, the consent requirement demands a carefully designed user-facing consent mechanism integrated into the product's setup and usage experience — typically a first-time setup wizard that presents the consent notice and captures the user's affirmative action, supplemented by accessible settings that allow

withdrawal of consent at any time.

The DPDPA provides for "deemed consent" in specified circumstances where the consent framework's requirements are considered met without an explicit consent action by the Data Principal: where the Data Principal has voluntarily provided personal data and it is clear from the circumstances that they consent to processing for the specified purpose; where processing is necessary for the performance of a function of the State or is required by law; where processing is necessary to protect the vital interests of the Data Principal or another person; and where processing is necessary for employment-related purposes or for a specified public interest function. The deemed consent provisions — particularly the "voluntarily provided" deemed consent — are likely to be relevant to electronics OEMs whose users actively interact with product features that collect personal data (such as a smart TV user who voluntarily uses a voice search function, implicitly consenting to voice data collection for that purpose). However, the boundaries of deemed consent are not precisely defined in the Act, and the implementing rules (which had not yet been finalised as of the Act's notification) are expected to clarify the specific circumstances in which deemed consent applies — a critical regulatory development that practitioners must monitor as the Act is operationalised.

1.3 Data Principals' Rights and Fiduciary Obligations

The DPDPA vests Data Principals with several fundamental rights regarding their personal data: the right of access to information about their personal data being processed by a Data Fiduciary; the right of correction and erasure of personal data that is inaccurate, incomplete, or no longer necessary for the purpose for which it was processed; the right to withdraw consent for processing (with prospective effect — withdrawal does not affect processing already completed with prior consent); the right to grievance redressal through the Data Fiduciary's complaint mechanism; and the right to nominate a representative to exercise these rights in the event of death or incapacity. Data Fiduciaries are obligated to: implement appropriate technical and organisational measures to ensure compliance with the Act; establish a clear and accessible grievance redressal mechanism accessible to Data Principals; not retain personal data beyond the period necessary for the specified processing purpose; and ensure that Data Processors acting on their behalf comply with all applicable data protection obligations. For electronics OEMs, the data retention limitation obligation — requiring deletion of personal data that is no longer necessary for the processing purpose — is a significant data governance challenge for products that collect and store usage analytics, device telemetry, and diagnostic data over extended product lifetimes.

1.4 Data Protection Board and Penalty Framework

The DPDPA establishes the Data Protection Board of India as the adjudicatory authority for complaints against Data Fiduciaries, with powers to investigate complaints, conduct inquiries,

and impose penalties. The Board is constituted by the Central Government (not as an independent statutory body) and exercises quasi-judicial functions through its Chairperson and Members, with proceedings conducted in a summary manner to enable expeditious resolution of data protection complaints. The penalty framework is tiered by the severity of the contravention: failure to take reasonable security safeguards resulting in a personal data breach — up to Rs. 250 crore; failure to notify the Board and affected Data Principals of a personal data breach — up to Rs. 200 crore; and violation of obligations relating to children's data or consent requirements — up to Rs. 200 crore. For major electronics companies, the potential penalties — up to Rs. 250 crore (approximately USD 30 million) — are significant but substantially lower than the GDPR's 4% of global annual turnover maximum, reflecting India's policy choice to impose proportionate rather than exemplary penalties in the initial phase of the DPDPA's implementation. The Board's decisions are appealable to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), providing a specialist technical appellate forum rather than routing appeals through the general High Court system.

CHAPTER TWO

CERT-In Directions 2022 and Cybersecurity Obligations

6-Hour Incident Reporting, Log Retention Requirements, VPN and Cloud Obligations, NCIIPC and Critical Infrastructure

> *The Indian Computer Emergency Response Team's (CERT-In) directions of April 2022 impose mandatory cybersecurity incident reporting, log retention, and information security obligations on a wide range of entities in the technology and electronics sector — creating compliance obligations that extend well beyond traditional IT companies to encompass electronics manufacturers, data centre operators, and cloud service providers.*

2.1 CERT-In Directions: Scope and Mandatory Obligations

CERT-In (the Indian Computer Emergency Response Team), constituted under Section 70B of the Information Technology Act, 2000, issued mandatory Directions in April 2022 that significantly expanded cybersecurity compliance obligations for technology companies operating in India. The Directions apply to "service providers, intermediaries, data centres, body corporates and government organisations" — a scope that encompasses electronics OEMs with connected product backends, cloud service providers hosting Indian data, virtual private network (VPN) providers, virtual asset service providers, and any other entity that operates IT systems processing personal data or communications data of Indian users. The primary obligations under the CERT-In Directions 2022 include: mandatory reporting of specified cybersecurity incidents (including data breaches, ransomware attacks, denial-of-service attacks, phishing attacks, and website defacements) to CERT-In within 6 hours of "noticing" the incident — one of the most aggressive reporting timelines in any jurisdiction's cybersecurity regulation globally; mandatory retention of IT and communications logs for a period of 180 days within Indian jurisdiction; mandatory synchronisation of all ICT system clocks with the Indian Standard Time servers maintained by NTP servers; and mandatory registration and KYC record maintenance for users of VPN, virtual private server, and cloud services, with these records to be maintained for 5 years and made available to CERT-In on demand.

The 6-hour incident reporting requirement — 6 hours from "noticing" the incident, not 6 hours from the incident occurring or being contained — is the most operationally challenging provision of the CERT-In Directions for large technology companies with complex, globally distributed infrastructure. In practice, "noticing" a cybersecurity incident at a large enterprise involves: automated detection by security monitoring systems (SIEM, EDR, network IDS); alert triage by the security operations centre (SOC) to distinguish genuine incidents from false positives; preliminary investigation to confirm the incident and assess its scope; executive escalation; and

legal and regulatory notification assessment. Completing this process and submitting the CERT-In notification within 6 hours of the initial detection event — including during nights, weekends, and holiday periods — requires: 24x7 SOC operations with India-specific incident response protocols; automated incident notification workflows integrated with the CERT-In reporting portal; pre-approved notification templates for different incident categories; and clear escalation paths that bypass normal business-hours approval processes when the 6-hour clock is running. Electronics OEMs with cloud-connected product backends — smart TVs, smart speakers, connected appliances — must design their incident response programmes to address CERT-In's 6-hour requirement as a specific operational standard rather than a general best-practice aspiration.

2.2 Log Retention: 180 Days in India

The CERT-In Directions require covered entities to maintain logs of ICT systems, including all application, database, network, operating system, and security device logs, for a minimum of 180 days "within Indian jurisdiction." The "within Indian jurisdiction" requirement — requiring that logs be stored on infrastructure physically located in India — is a de facto data localisation requirement for cybersecurity log data, distinct from any DPDPA localisation requirements, and may require entities who currently store logs in international cloud infrastructure (such as AWS, Azure, or Google Cloud data centres outside India) to either migrate their India-specific logs to Indian data centres or establish separate log storage infrastructure in India. For electronics OEMs with connected product fleets — devices that generate log data across the lifecycle of consumer use — the 180-day log retention requirement creates storage infrastructure obligations proportional to the volume of the Indian device fleet and the log verbosity of each device's backend system. The practical compliance investment for a large electronics OEM with millions of connected Indian devices can be substantial, particularly for companies that did not previously maintain India-specific log retention infrastructure.

2.3 NCIIPC and Critical Information Infrastructure

The National Critical Information Infrastructure Protection Centre (NCIIPC), designated under Section 70A of the IT Act 2000 as the nodal agency for protection of critical information infrastructure in India, is relevant to electronics sector companies whose systems or products underpin critical infrastructure operations: telecommunications equipment manufacturers, industrial electronics providers for power, transport, and financial systems, and defence electronics suppliers. NCIIPC maintains a taxonomy of "Critical Information Infrastructure" — the computer resources whose incapacitation or destruction would have a debilitating impact on national security, economy, public health, or safety — and coordinates with sectoral regulators to ensure that critical infrastructure operators implement appropriate security controls. Electronics companies whose products are classified as critical information infrastructure components (such as telecom base station equipment, industrial control system electronics, or

power grid monitoring systems) are subject to NCIIPC's guidelines for critical infrastructure protection, which include: mandatory security audits by empanelled NCIIPC auditors; mandatory reporting of cybersecurity incidents affecting critical infrastructure to NCIIPC within specified timelines; and compliance with NCIIPC's technical standards for secure development practices for critical infrastructure electronics. The interaction between CERT-In's generally applicable incident reporting requirements and NCIIPC's critical infrastructure-specific requirements creates a dual reporting obligation for electronics companies in the critical infrastructure space — a compliance complexity that requires clear internal protocols specifying when each authority must be notified and in what sequence.

CHAPTER THREE

IT Act 2000: Electronics Sector Obligations

Section 43A, SPDI Rules 2011, Computer-Related Offences, Intermediary Liability and Electronic Contracts

3.1 Section 43A and SPDI Rules: Reasonable Security Practices

Section 43A of the Information Technology Act, 2000 (inserted by the IT Amendment Act, 2008) imposes civil liability on body corporates — including all companies and organisations that handle personal data — for failure to implement and maintain "reasonable security practices and procedures" when dealing with "sensitive personal data or information" (SPDI). The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), notified under Section 43A, define SPDI to include: passwords; financial information (bank account, credit/debit card details); physical, physiological, and mental health conditions; sexual orientation; medical records; and biometric data. The SPDI Rules require body corporates to: maintain a documented privacy policy accessible to users specifying the type of data collected, its use, disclosure, and security practices; collect SPDI only with the data subject's consent and for lawful purposes; not retain SPDI longer than necessary; allow data subjects to review and correct their SPDI; implement reasonable security practices (aligned with IS/ISO 27001 or an internationally recognised standard); and obtain prior consent before disclosing SPDI to third parties. For electronics companies, the SPDI Rules are particularly relevant for: products with biometric capabilities (fingerprint sensors, facial recognition cameras); health monitoring wearables (which collect health data covered by the SPDI definition); payment-enabled devices (which may process financial information); and connected products that collect and transmit location, health, and usage data to backend servers.

3.2 Computer-Related Offences Relevant to Electronics Sector

The IT Act 2000 defines several computer-related offences that have direct relevance to electronics manufacturers and their products. Section 65 criminalises tampering with computer source documents — relevant to electronics companies whose devices run proprietary embedded software protected as source code (any deliberate alteration or concealment of source code of computer programmes, computer systems, or computer networks is a criminal offence punishable with imprisonment up to 3 years). Section 66 criminalises computer-related offences such as hacking — relevant for security researchers who discover vulnerabilities in electronic products and need to manage responsible disclosure without inadvertently violating Section 66. Section 66E criminalises violation of privacy through the unauthorised capture, publication, or transmission of private images — relevant for electronics companies whose products include cameras or image capture capabilities (the obligation to ensure that product design does not

facilitate privacy violations through features that enable capture or transmission of images without the subject's knowledge). Section 69 empowers the Central Government to intercept, monitor, or decrypt information transmitted through any computer resource for purposes of national security — relevant for electronics manufacturers whose products include encryption, VPN, or secure communication capabilities, who must ensure their products can comply with Section 69 decryption orders where legally required.

3.3 Intermediary Liability Framework: IT Rules 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 — commonly known as the IT Rules 2021 — establish a detailed framework of obligations for "intermediaries" (entities that host or transmit third-party content) with significant implications for electronics companies who operate digital platforms, marketplaces, or communication services embedded in or associated with their products. Significant Social Media Intermediaries (SSMIs) — intermediaries with user bases above 5 million registered users in India — face enhanced obligations including: appointment of a Chief Compliance Officer resident in India; appointment of a Nodal Contact Person for law enforcement coordination; appointment of a Grievance Officer resident in India; publication of monthly compliance reports; and provision of a mechanism for voluntary "verification" of user accounts. For electronics companies that operate large consumer-facing digital platforms (app stores, cloud services, media streaming services integrated with electronics products), the SSMI designation and its associated obligations create significant compliance investment requirements and India-specific governance infrastructure obligations. The IT Rules 2021 also require all intermediaries to publish terms of use and privacy policies, implement due diligence practices for user activity, and cooperate with government requests for information about users — obligations that affect the design of electronics companies' digital service infrastructure in India.

CHAPTER FOUR

Cross-Border Data Flows and Localisation

DPDPA Transfer Framework, RBI Payment Data Localisation, Telecom Data Governance and International Adequacy

4.1 DPDPA Cross-Border Transfer Framework

The DPDPA 2023's approach to cross-border personal data transfers is significantly more permissive than the data localisation mandates that characterised earlier draft Indian data protection bills. Rather than requiring personal data to be stored within India, the DPDPA allows cross-border transfers of personal data to countries that the Central Government notifies as permissible transfer destinations (a "whitelist" approach) and prohibits transfers to countries that are specifically notified as impermissible transfer destinations (a "blacklist" approach for jurisdictions of concern). This whitelist/blacklist framework, to be operationalised through the DPDPA Rules that the Central Government will notify, gives the government flexibility to calibrate transfer permissions country-by-country based on the adequacy of the destination country's data protection framework, geopolitical considerations, and reciprocity of data governance standards. For electronics companies with global cloud infrastructure — where data flows routinely occur across multiple jurisdictions as part of normal service delivery — the DPDPA's transfer framework means that existing global data transfer architectures may need adaptation to ensure that Indian personal data does not flow to blacklisted jurisdictions, and that proper legal mechanisms are in place for transfers to countries not yet on the whitelist.

4.2 RBI Payment Data Localisation

The Reserve Bank of India's data localisation mandate for payment system data — requiring that all data related to payment transactions of Indian customers be stored exclusively on servers located within India — has been in force since October 2018, when the RBI's circular on "Storage of Payment System Data" required all payment system operators to store Indian payment data domestically within six months. The RBI localisation mandate covers: the full end-to-end transaction details including customer data, payment credentials, transaction details, and merchant data; and any processing of such data, whether by the payment system operator or its third-party processors. For electronics companies whose products include embedded payment capabilities — NFC-enabled smartphones for contactless payments, smartwatches with payment features, point-of-sale terminals — the RBI payment data localisation mandate requires that the backend payment processing infrastructure for Indian transactions is hosted in India, separately from the global payment infrastructure. This localisation requirement has driven significant infrastructure investment by international payment networks (Visa, Mastercard, American Express) and payment system operators in India-based data centre capacity, and electronics

OEMs whose products integrate these payment capabilities must ensure their product architectures route Indian transaction data to the compliant localised infrastructure.

4.3 Telecom Data Governance Under the Telecom Act 2023

The Telecommunications Act, 2023 — which received Presidential assent in December 2023 and replaces the Indian Telegraph Act, 1885 — introduces a new framework for telecom data governance with direct implications for electronics companies whose products incorporate wireless communications capabilities. Section 22 of the Telecom Act 2023 addresses privacy and security of telecommunications, requiring telecom entities to implement appropriate technical and organisational measures to safeguard the privacy of messages and the security of telecommunications networks, and providing the government with powers to specify standards, procedures, and conditions for ensuring security of telecommunications infrastructure. The Telecom Regulatory Authority of India (TRAI) will play a central role in developing the implementing regulations under the Telecom Act 2023, including data governance standards for telecom networks. For electronics companies manufacturing telecom terminal equipment (smartphones, Wi-Fi routers, modems, base stations), the Telecom Act 2023's security and privacy provisions create a regulatory overlay that supplements the BIS CRS compliance and WPC type approval requirements with additional security obligations that must be addressed in product design and network integration.

CHAPTER FIVE

Sectoral Obligations: IoT, Smart Products and OEM Compliance

MEITY IoT Guidelines, Connected Device Security, OTA Update Obligations and Smart Product Data Governance

5.1 MEITY IoT Security Guidelines

The Ministry of Electronics and Information Technology has issued guidelines on information security practices for the Internet of Things (IoT) ecosystem in India, providing a non-binding but commercially significant framework for security practices that electronics OEMs are expected to implement in connected products. The MEITY IoT security guidelines — which draw on the ETSI EN 303 645 standard (the European baseline security standard for consumer IoT) and the UK's Code of Practice for Consumer IoT Security — specify baseline security requirements including: no universal default passwords (every device must use a unique password or require the user to set one before operation); implementation of a vulnerability disclosure policy enabling security researchers to report discovered vulnerabilities; regular security updates with a published support period indicating how long the device will receive security patches; secure storage of sensitive security parameters (cryptographic keys, credentials) in hardware security elements; minimisation of exposed attack surfaces (no open ports, disabled services, and interfaces that are not needed); integrity of software and firmware using cryptographic verification to prevent installation of unauthorized code; protection of personal data using end-to-end encryption for data in transit and secure storage for data at rest; device resilience against denial-of-service attacks; and monitoring of system telemetry data with anomaly detection capabilities. These guidelines have been issued as advisories rather than mandatory regulations, but MEITY has signalled its intention to progressively make IoT security requirements mandatory for specific product categories, starting with connected baby monitors, security cameras, smart doorbells, and other products with direct safety or privacy implications.

5.2 Connected Consumer Electronics: Data Governance Framework

Connected consumer electronics — smart TVs, smart speakers, smart home automation devices, wearable health trackers, and connected appliances — collect large volumes of personal and behavioural data from Indian users as part of their core functionality. The data governance obligations for these products' manufacturers encompass: DPDPA compliance (consent for personal data collection, retention limitation, data principal rights fulfilment); CERT-In compliance (6-hour incident reporting, 180-day log retention for backend systems); SPDI Rules compliance (reasonable security practices for any health or biometric data collected); and BIS CRS compliance (product safety certification before sale). For smart TVs specifically, TRAI's

Telecom Commercial Communications Customer Preference Regulations apply to any behavioural advertising based on viewing data — placing regulatory constraints on the commercial use of viewership analytics for targeted advertising. For health wearables that track physiological parameters (heart rate, SpO2, ECG, blood glucose), the interaction between DPDPA's protections for health data and the SPDI Rules' treatment of health information as sensitive data creates a particularly demanding compliance environment, as health data breaches can have severe consequences for individuals' privacy, insurance-worthiness, and employment prospects that justify the heightened regulatory scrutiny.

5.3 OTA Software Update Obligations

Electronics manufacturers who provide Over-the-Air (OTA) software and firmware updates to connected products have specific legal obligations related to the security, transparency, and consumer consent implications of OTA updates. While India does not yet have a dedicated OTA update regulation (unlike the automotive sector where MoRTH is developing OTA guidance for connected vehicles), the general legal framework creates the following OTA obligations for electronics OEMs: DPDPA consent requirements apply where an OTA update modifies the product's data collection practices — introducing a new data collection feature or changing the privacy settings requires fresh consent from the Data Principal, and the OTA update process must be designed to capture this consent before the new functionality activates; consumer protection obligations under the CPA 2019 require that OTA updates do not materially degrade product performance in ways that were not disclosed to the consumer at purchase — updates that reduce battery capacity, processor performance, or camera functionality through software throttling without consumer consent could constitute an unfair trade practice; and BIS CRS compliance requires that OTA updates do not take a product outside its certified specification — an OTA update that introduces a Wi-Fi frequency band not covered by the product's WPC type approval, for example, would create a compliance gap that requires a fresh regulatory approval before the update can be deployed to Indian devices.

> **Booklet V Key Takeaways:** India's data protection and cybersecurity regulatory framework for electronics companies spans four primary legal instruments: the DPDPA 2023 (consent, data principal rights, cross-border transfers, Data Protection Board penalties up to Rs. 250 crore); CERT-In Directions 2022 (6-hour incident reporting, 180-day log retention in India); IT Act 2000 and SPDI Rules (reasonable security practices for sensitive personal data, computer-related offences, intermediary liability); and emerging IoT security standards and connected device regulations. The combination creates a demanding compliance environment that requires integrated legal expertise across data protection, cybersecurity, consumer protection, and product safety to provide commercially effective legal counsel for electronics companies in India.

EXTENDED ANALYSIS

Data Protection and Cybersecurity: Implementation Framework

DPDPA Rules Development, Incident Response Architecture, Privacy Engineering, AI Governance and Global Compliance

E.1 DPDPA Rules: Anticipated Provisions and Industry Implications

The Digital Personal Data Protection Act, 2023 delegates significant rule-making authority to the Central Government for operationalising the Act's framework — the "DPDPA Rules" that the Ministry of Electronics and Information Technology will notify are expected to address: the specific conditions and procedures for cross-border data transfers (specifying the whitelist of permissible destination countries and the documentation required for lawful transfers); the qualifications and appointment requirements for Data Protection Officers for Significant Data Fiduciaries; the form and manner of consent notices (including language and accessibility requirements); the procedure for exercising Data Principal rights (access, correction, erasure, and grievance redressal timelines); the qualifications for Data Auditors; the methodology for conducting Data Protection Impact Assessments; and the specific security standards that constitute "reasonable security practices" for different categories of personal data and different categories of Data Fiduciaries. For electronics companies, the most commercially significant anticipated rules are those governing: the consent notice requirements (which will determine the user interface design changes required for connected products' setup and settings experiences); the cross-border data transfer framework (which will determine whether existing global cloud infrastructure can be used for Indian data without localisation); and the breach notification requirements (which will specify the information to be reported to the Data Protection Board within the specified reporting window). Companies should monitor the MEITY consultation process for DPDPA Rules closely, as the rules' content will determine the practical compliance investment required by the electronics sector — an investment that could range from modest (if the rules adopt a flexible, principles-based approach) to very substantial (if the rules require specific technical measures, local infrastructure, or extensive administrative processes).

The Data Protection Board's enforcement approach — which will be shaped by the Board's first significant investigations and decisions — will define the practical compliance risk of DPDPA non-compliance for electronics companies. The DPDPA's tiered penalty structure (up to Rs. 250 crore for security breaches, Rs. 200 crore for notification failures) is designed to be proportionate and persuasive rather than exemplary, but the specific factors that the Board will consider in determining penalty levels (the severity of the breach, the number of affected Data Principals, the sensitivity of the data involved, the proactive measures taken by the company to mitigate harm, and the company's compliance programme at the time of the breach) are not fully

specified in the Act and will need to be developed through the Board's case law. International comparison suggests that data protection enforcement bodies typically focus initial enforcement action on the largest and highest-profile companies, whose data practices affect the most consumers and whose enforcement actions generate the most public and regulatory impact. For major electronics companies with large Indian consumer data footprints — global smartphone OEMs, connected device manufacturers, and digital service providers — the DPDPA enforcement risk is therefore elevated relative to smaller companies, justifying the investment in comprehensive compliance programmes that can demonstrate good-faith compliance efforts to the Board if a data security incident occurs.

E.2 Privacy Engineering for Connected Electronics

Privacy engineering — the systematic integration of data protection principles and technical privacy safeguards into the design and development of electronic products — is the foundation of DPDPA compliance for electronics OEMs whose products collect and process personal data. Privacy engineering in the context of connected electronics encompasses: data minimisation (designing products to collect only the data categories strictly necessary for the product's core functions, and not collecting convenience data that adds limited value relative to the privacy cost); privacy by default (configuring new product setups to enable only the minimum necessary data collection by default, requiring active user choice to enable additional collection); purpose limitation (designing data processing architectures that technically enforce the limitation of collected data to its specified purpose, preventing data collected for one function from being accessible to or used by another function); storage limitation (designing automatic data deletion or anonymisation workflows that delete personal data when the retention period specified in the DPDPA consent expires); and security by design (building security controls — encryption, access controls, authentication — into the product architecture from the earliest design stage rather than adding them as afterthoughts). The "privacy by design" principles developed by Ann Cavoukian (and now reflected in GDPR Article 25 and anticipated in DPDPA Rules) are directly applicable to electronics product development, and companies whose product development methodology incorporates Privacy Impact Assessments at key design gate reviews are demonstrably better positioned to achieve DPDPA compliance at product launch than those that treat privacy as a post-development compliance check.

E.3 AI and Machine Learning in Electronics: Emerging Governance

Artificial intelligence and machine learning technologies are increasingly embedded in consumer electronics: smartphone cameras use AI for scene recognition, portrait mode, and night photography; smart speakers use AI for voice recognition and natural language understanding; smart TVs use AI for content recommendation; wearables use AI for health metric analysis and anomaly detection; and home automation systems use AI for energy optimisation and predictive maintenance. These AI applications create both remarkable consumer experiences and

significant data governance challenges — AI models trained on personal data require large volumes of training data, create outputs that can reflect biases in training data, and generate decisions (such as content recommendations, health risk assessments, or access control decisions) whose basis may not be explainable to affected users. India's AI governance framework is currently under development, with MEITY's draft framework on "Responsible AI" (released for consultation in 2023) and the Digital India Act (which will replace the IT Act 2000 and will include AI governance provisions) expected to create mandatory requirements for the use of AI in consumer electronics contexts. For electronics OEMs who deploy AI-driven features in their products, the emerging AI governance framework creates compliance obligations around: the use of training data (consent for use of personal data in AI training; fairness and bias assessment for AI models); the transparency of AI decisions (explanations for AI-generated outputs that affect users); and the human oversight of AI systems (requirements to provide users with the option of human review of significant AI-driven decisions). Companies that invest in responsible AI practices today — including bias testing, explainability documentation, and user-facing transparency about AI use — will be better positioned for regulatory compliance when mandatory requirements take effect.

E.4 Global Cybersecurity Compliance: Multi-Jurisdiction Management

Electronics companies with global operations must manage cybersecurity compliance across multiple jurisdictions simultaneously — a multi-framework challenge that requires an integrated compliance approach rather than jurisdiction-by-jurisdiction compliance silos. The major jurisdictional cybersecurity frameworks relevant to electronics companies with India operations include: India's CERT-In Directions (6-hour incident reporting, 180-day India log retention); the EU's NIS2 Directive (24-hour early warning and 72-hour initial notification for cybersecurity incidents affecting entities in EU critical sectors); the US SEC cybersecurity disclosure rules (4-business-day disclosure of material cybersecurity incidents for SEC-reporting companies); China's Multi-Level Protection Scheme (MLPS) for cybersecurity of information systems; and Singapore's Cybersecurity Act (6-hour notification for major cybersecurity incidents affecting critical information infrastructure). The challenge of harmonising incident response timelines across these frameworks — where India requires 6-hour notification, the EU requires 24-hour early warning, the US requires 4-business-day disclosure for material incidents, and Singapore requires 6-hour notification for CII incidents — requires electronics companies to design their incident response programmes around the most stringent timeline (India's 6-hour requirement) and to ensure that multi-jurisdictional notification obligations are addressed in parallel rather than sequentially. The practical implementation of a globally harmonised incident response programme — with 24x7 SOC coverage, pre-cleared multi-jurisdictional notification templates, and cross-functional escalation processes that respect each jurisdiction's specific requirements — is among the most complex operational compliance investments for global electronics companies with significant India operations.

Booklet V — Complete Summary: India's data protection and cybersecurity regulatory framework for electronics is a dynamic and evolving compliance environment spanning the DPDPA 2023, CERT-In Directions 2022, IT Act 2000, and emerging IoT and AI governance frameworks. The convergence of these instruments creates layered compliance obligations for electronics companies that require privacy engineering embedded in product design, robust incident response capabilities meeting the 6-hour CERT-In reporting timeline, comprehensive data governance for connected products, and proactive engagement with the evolving DPDPA Rules and Digital India Act development. Electronics companies that treat data protection and cybersecurity as integral product design requirements — rather than afterthought compliance checkboxes — will not only achieve regulatory compliance but will build consumer trust and brand differentiation in an increasingly privacy-aware Indian market.