BoardMatters Forum

Digital Personal Data Protection Act (DPDPA)

04 December 2025

The better the question. The better the answer.
The better the world works.

Shape the future with confidence

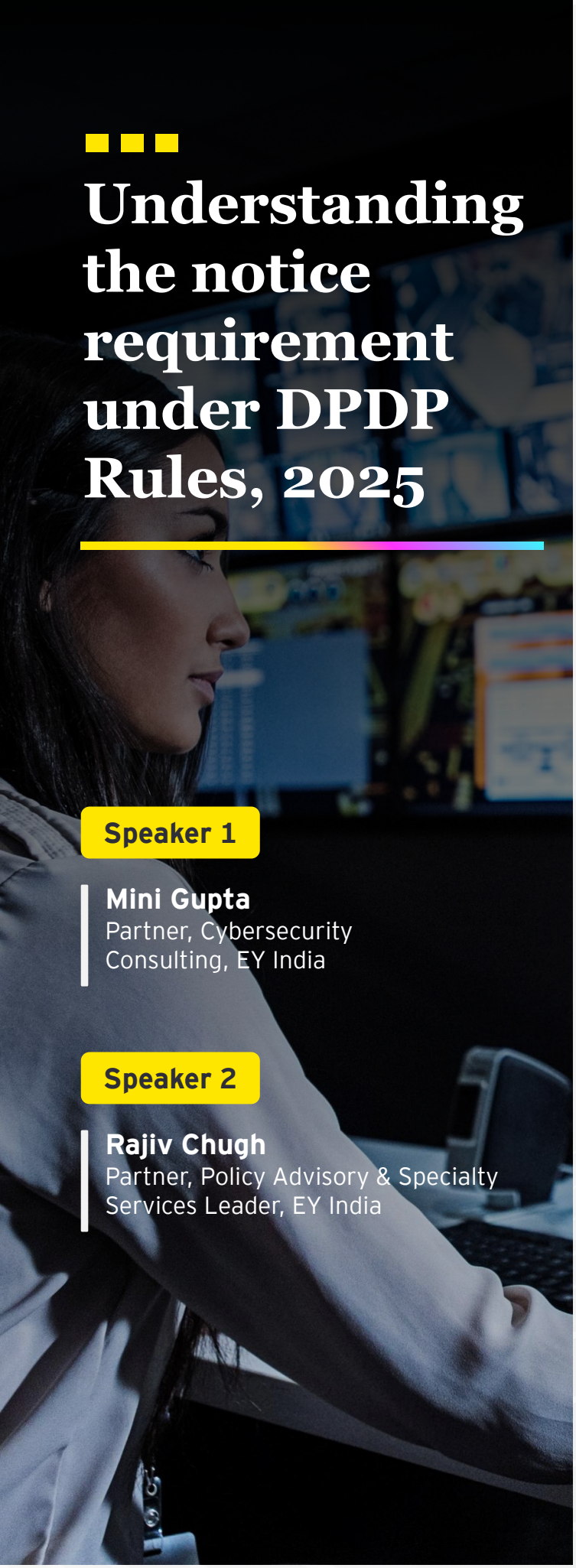
Introduction

On 4 December 2025, EY India organized the BoardMatters Forum (BMF) as part of its continuing dialogue with business leaders on governance and regulatory change. The forum witnessed the presence of 27 independent directors who shared their views on data protection preparedness under the Digital Personal Data Protection Act.

The discussions commenced with a conversation on "DPDP Rules, 2025 – an overview," starting with notice requirements and then covering consent, the role of Consent Managers and the rights granted to Data Principals. The dialogue further touched upon data retention, security safeguards, the responsibilities of Data Fiduciaries and Data Processors, data breaches and the penalty framework. This set the foundation for the roadmap to enable compliance with the Act and its Rules, focusing on readiness planning, policy updates, consent workflows, breach-response mechanisms, and the importance of board oversight.

Even though the conversations spanned multiple aspects of the Act, the key understanding remained clear: Boards play an important role in shaping data governance, driving compliance maturity and supporting responsible handling of personal data across enterprises.

Understanding the notice requirement under DPDP Rules, 2025



Speaker 1

Mini Gupta
Partner, Cybersecurity Consulting, EY India

Speaker 2

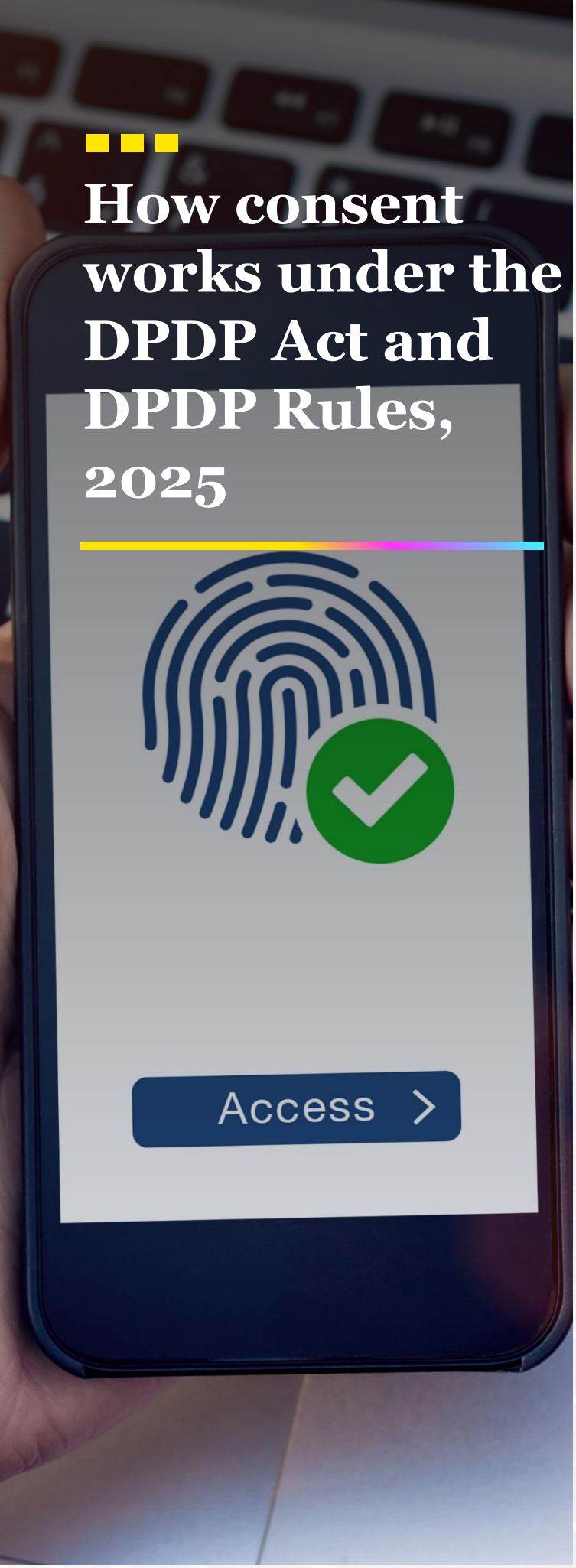
Rajiv Chugh
Partner, Policy Advisory & Specialty Services Leader, EY India

When a Data Fiduciary collects personal data, the first step is to provide a clear and accessible notice to the Data Principal. This explains what information the company wants, why and how it will be used. The notice must be written in simple language and presented independently rather than hidden inside lengthy documents or general terms. The intent is for individuals to know exactly what they are agreeing to, without confusion or ambiguity.

The rules state that a notice must contain an itemized description of the personal data being collected along with the specific purpose for processing, including any related service it supports. The notice must also provide a communication link that lets the Data Principal withdraw consent, exercise their rights under the Act, or file a complaint with the Data Protection Board of India (DPB) if required.

The notices have to be available in English, or in one of the 22 Indian languages, based on operational regions. Further, in cases where processing is already happening, retrospective consent notices must be shared before the law becomes fully enforceable. In short, the notice acts as the foundation for transparency and informed consent under the DPDP framework.

Board members are expected to oversee how organizations design, deliver and update privacy notices, along with the notices remaining clear, lawful and accessible across channels. Their role also includes monitoring compliance readiness, verifying consent processes, allocating resources and encouraging leadership accountability for rights-based communication with Data Principles.



How consent works under the DPDP Act and DPDP Rules, 2025

Consent stands at the core of personal data processing. Before collecting or using personal data, organizations have to seek approval from the Data Principal in a manner that is free, informed, specific and unambiguous. This means individuals should clearly know what they are agreeing to, for what purpose and how their data will be handled. A simple pre-ticked box or passive acceptance does not count. Instead, clear affirmative action is required, such as selecting an option or clicking an 'agree' button. As consent can also be revoked at any time, individuals should be able to withdraw without facing hurdles.

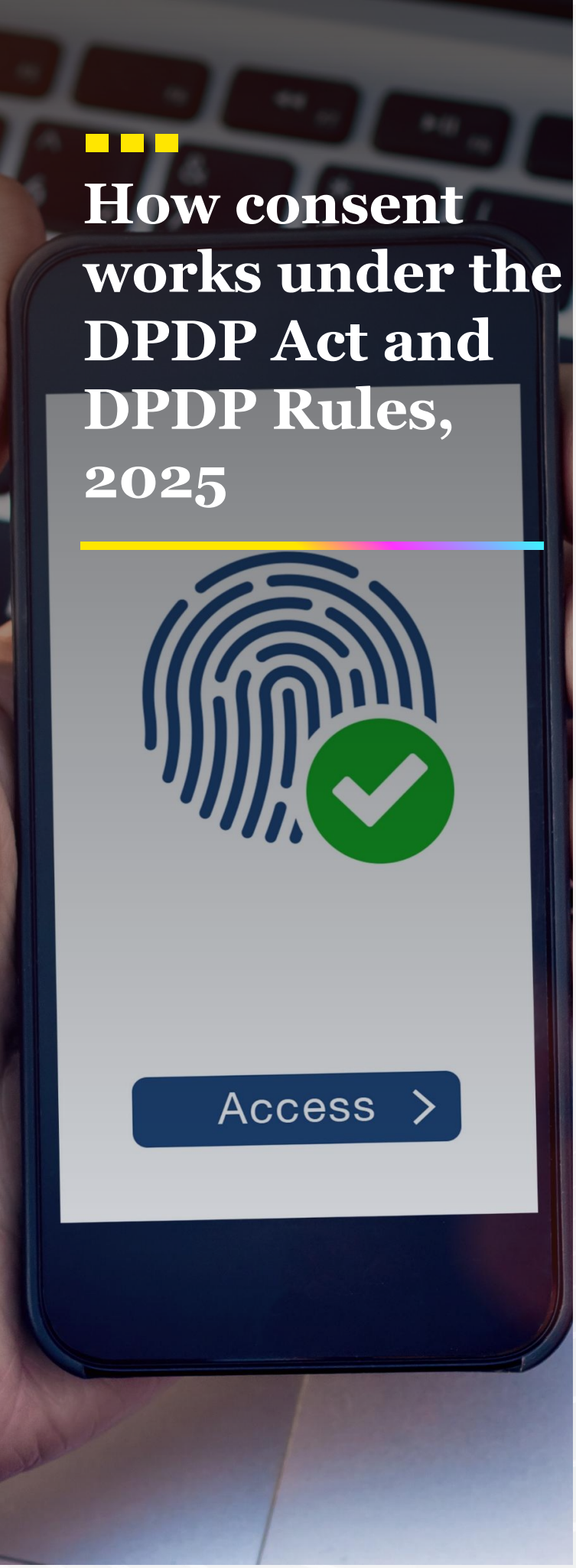
An important responsibility lies with the Data Fiduciary to verify whether historical personal data was collected with valid consent. If not, fresh consent needs to be requested.

However, the Act also lists situations where processing can occur without explicit consent, such as voluntary data submission by the Data Principal, life-threatening medical emergencies, the issuance of subsidies or certificates, legal compliance, situations of public safety or national security, disease outbreaks and employment-related requirements to safeguard the organization from risk or liability.

For data of children, companies need verifiable consent. Also:

- Data Fiduciary must verify the identity and age of a child.
- Guardian consent has to be confirmed through reliable proof.
- Verification can be based on documents or digital locker records.
- Technical and organizational controls should enable the validity of consent.
- No fresh consent needed for certain activities focused on child welfare.

How consent works under the DPDP Act and DPDP Rules, 2025



In simple terms, consent is the ethical and legal foundation of data use, but the law also recognizes exceptions where processing is essential for public interest or mandatory governance functions.

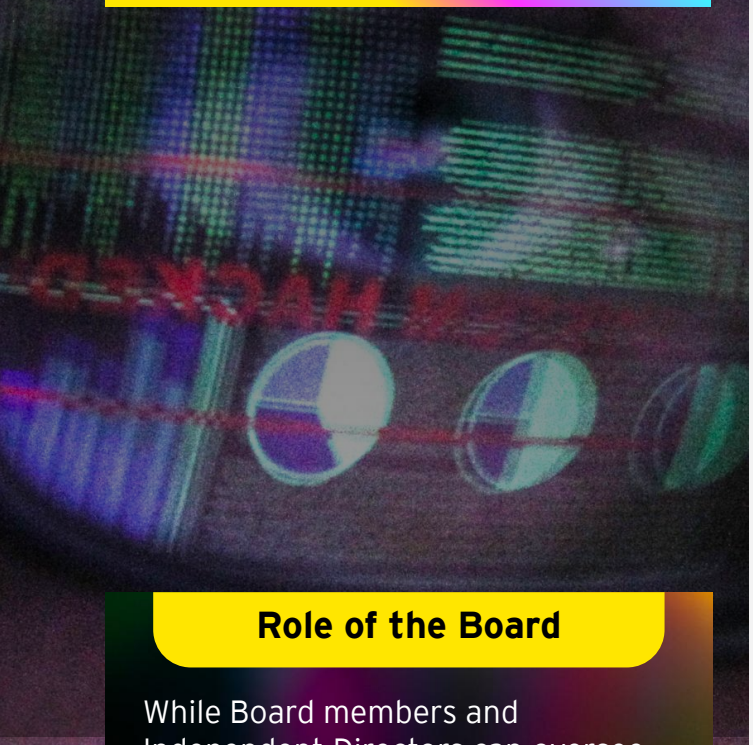
A Consent Manager plays an important role in enabling individuals to give, manage and withdraw consent through a secure and user-friendly platform. Their work helps create trust and clarity in consent-based data processing.

To be registered with the Data Protection Board of India (DPB), the entity must be incorporated in India with a minimum net worth of INR2 crore, have sound financial and management practices and demonstrate technical, operational and financial capacity. The platform should be interoperable and independently certified to meet data protection standards. After being registered, the Consent Manager has to keep consent actions transparent and machine-readable, safeguard personal data, maintain audit trails and records for at least seven years or as required.

Role of the Board

Independent Directors and Board members are expected to oversee how consent mechanisms operate within the organization such that consent collection is lawful, transparent and user-friendly, periodically review compliance reports, and verify that historical data has valid consent records. They can guide the management in appointing Consent Managers where necessary, monitor breach-response readiness and adopt policies that reflect the rights of Data Principals. The Board can provide a layer of governance so that consent is not just a formality, but a continuous responsibility backed by accountability and ethical practices.

Data Principal rights, security safeguards and retention responsibilities



The DPDP Rules, 2025, grant Data Principals several rights that strengthen control over their personal information. Individuals have the right to access details of data being processed, understand its purpose and request copies where required. They may also seek correction or erasure. They can access grievance redressal and organizations must publish clear timelines for addressing such concerns, not exceeding 90 days. Data Principals can also withdraw consent at any time and nominate one or more persons to exercise rights on their behalf in case of disability or incapacity. This framework reinforces transparency, agency and informed participation in data interactions.

On the security front, Data Fiduciaries must implement measures to safeguard personal data across its lifecycle. These include:

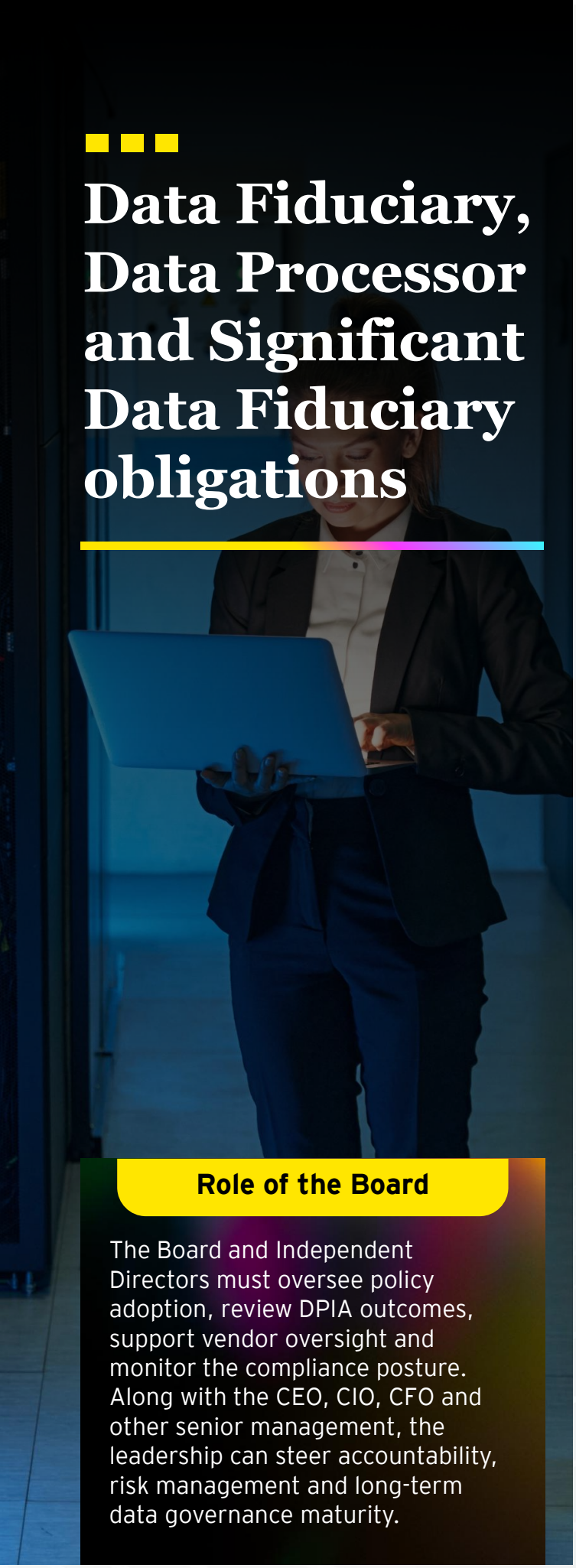
- Encryption and masking
- Strong access control
- Explicit security clauses in vendor contracts
- Technical and organizational measures to handle threats

Backup and restoration protocols, along with logging and monitoring capabilities, build resilience and traceability. Data retention rules require personal and traffic data to be stored for at least one year, after which it must be erased unless required for legal, operational, or regulatory reasons. For high-scale entities such as ecommerce platforms with over two crore users, online gaming intermediaries with more than 50 lakh users and social media intermediaries crossing two crore users, certain data categories must be deleted within three years of the last interaction. Data Principals must also be informed 48 hours before deletion.

Role of the Board

While Board members and Independent Directors can oversee policy implementation, risk controls and grievance transparency, the CIO must focus on robust security architecture, compliance monitoring and breach readiness. The CFO would need to allocate budgets for cybersecurity, audits and technology upgrades. Financial readiness may be required for compliance investments and penalties. Together, the Board and senior management can drive accountability and sustained adherence to the DPDP Act.

Data Fiduciary, Data Processor and Significant Data Fiduciary obligations



Under the DPDP Rules, 2025, a Data Fiduciary is responsible for determining the purpose and manner of personal data processing. Core responsibilities include enabling compliance with DPDP requirements, maintaining accurate and secure personal data with proper controls and publishing contact details of the Data Protection Officer or authorized grievance contact. They must honor consent withdrawal, enable access requests and provide grievance redressal mechanisms. Additionally, Data Fiduciaries have to put clear contracts in place for all Data Processors, defining responsibilities and security expectations. Due diligence is crucial, as they must assess processors regularly to confirm adherence to privacy standards and legal obligations.

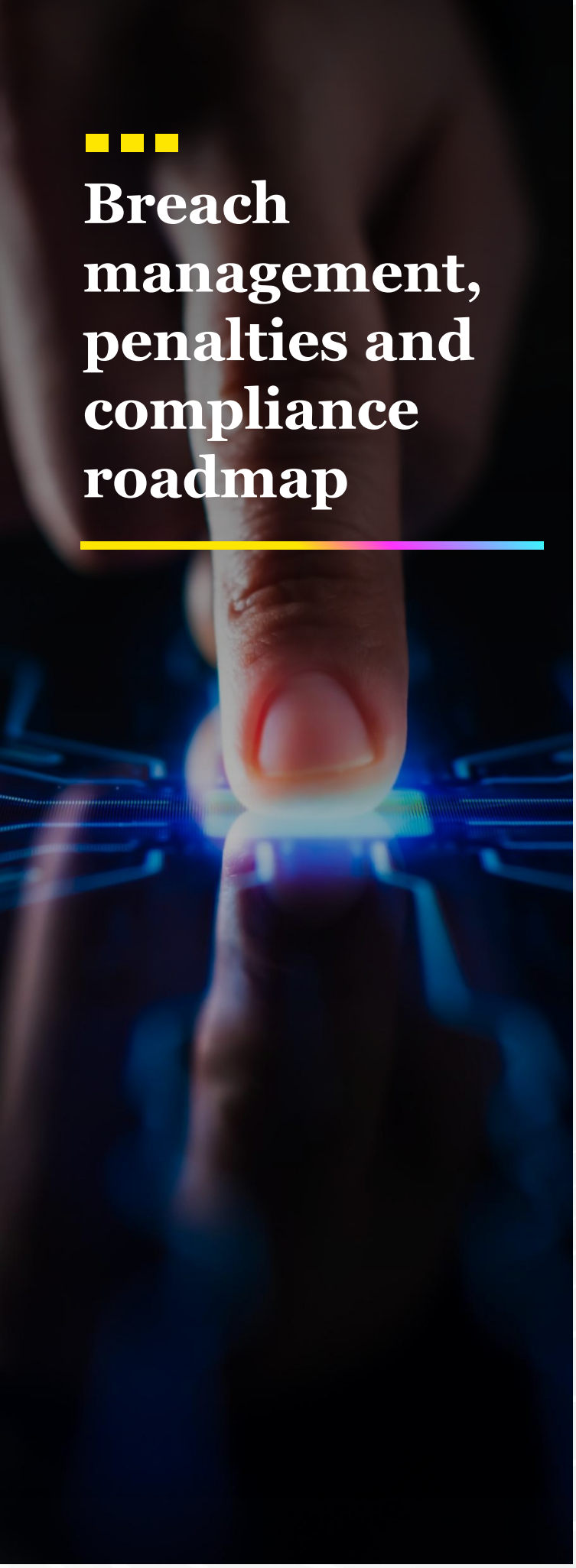
Data Processors operate on behalf of the Data Fiduciary and process data only as per instructions and contract terms. They must establish strong data protection standards, enable confidentiality and support breach reporting. The fiduciary must enable processors to meet compliance thresholds through periodic evaluation, monitoring and contractual accountability.

Certain entities may be classified as Significant Data Fiduciaries (SDFs) by the government based on factors such as the sensitivity and volume of the data processed, risk to individuals' rights, impact on national sovereignty, electoral democracy, state security and public order. Once designated, SDFs carry additional obligations:

- Conduct annual Data Protection Impact Assessments (DPIA)
- Submit audit findings to the Data Protection Board of India (DPB)
- Review automated decision-making systems
- Comply with restrictions on cross-border data transfers

Role of the Board

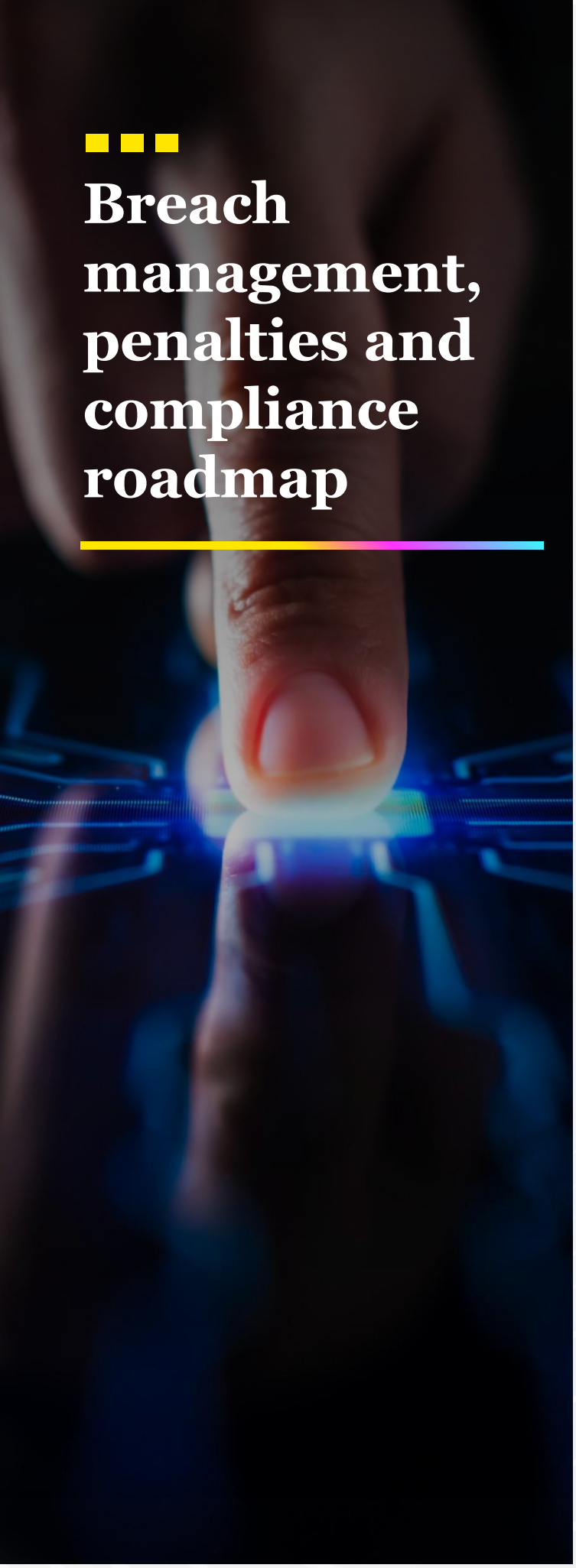
The Board and Independent Directors must oversee policy adoption, review DPIA outcomes, support vendor oversight and monitor the compliance posture. Along with the CEO, CIO, CFO and other senior management, the leadership can steer accountability, risk management and long-term data governance maturity.



Breach management, penalties and compliance roadmap

A personal data breach triggers a structured and time-sensitive response under the DPDP Rules, 2025. The process begins when an organization becomes aware of a breach.

1. The breach must be investigated immediately to understand its nature, cause and extent.
2. Once preliminary details are known, the Data Fiduciary must notify the Data Principal without delay, outlining the description of the breach, the type of data involved, potential consequences, measures taken, safety steps the individual can take and valid contact details for support.
3. Parallelly, the Data Fiduciary must notify the Data Protection Board of India (DPB) without delay, providing factual details of the incident, measures taken or proposed, findings around the cause, investigation outcomes and remediation steps.
4. Within 72 hours, or within a DPB-approved extended timeline, the Data Fiduciary must submit a detailed breach report, demonstrating accountability and transparency.



Breach management, penalties and compliance roadmap

Penalties for non-compliance are substantial. Failure to implement reasonable security safeguards may attract up to INR250 crore, while delay or failure in breach notification can cost up to INR200 crore. Non-compliance with child-specific requirements may also draw penalties of up to INR200 crore. Significant Data Fiduciaries face up to INR150 crore for additional obligation breaches and general violations of the Act can lead to INR50 crore fines. A Data Principal may also be penalized up to INR10,000 for misuse of their rights. Importantly, cumulative penalties may reach INR850 crore, highlighting the seriousness of data governance.

To help organizations mature compliance practices, a clear roadmap is recommended.

1. Start with a privacy control matrix, followed by a current-state assessment and data discovery/classification.
2. Next comes design and documentation, including notices, consent workflows and third-party governance.
3. Implementation involves technical safeguards, Data Privacy Impact Assessments (DPIA), the setup of a privacy office, vendor controls and security measures.
4. Subsequently, audit and review cycles help refine controls and privacy-enhancing technologies (PETs) support continuous optimization.

Role of the Board

Boards and independent directors can guide companies on breach governance, oversee reporting discipline and support accountability. Measures such as the review of DPIAs, breach dashboards and readiness plans can go a long way in establishing data protection. A mature privacy culture is essential to reduce breach impact and safeguard trust.

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

EYIN2604-019
ED None

JS

ey.com/en_in

@EY_India EY EY India EY Careers India @ey_indiacareers