

Section 2 DPDPA

Definitions. 2. In this Act, unless the context otherwise requires,—

- (a) “Appellate Tribunal” means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997; (b) “automated” means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data; (c) “Board” means the Data Protection Board of India established by the Central Government under section 18; (d) “certain legitimate uses” means the uses referred to in section 7; (e) “Chairperson” means the Chairperson of the Board; (f) “child” means an individual who has not completed the age of eighteen years; (g) “Consent Manager” means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform; (h) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means; (i) “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data; (j) “Data Principal” means the individual to whom the personal data relates and where such individual is—
- (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf; (k) “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary; (l) “Data Protection Officer” means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10; (m) “digital office” means an office that adopt

[recovered from the vector store — section2.html p.2]

s an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

- (n) “digital personal data” means personal data in digital form;
- (i) a gain in property or supply of services, whether temporary or permanent; or
- (ii) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;
- (i) a loss in property or interruption in supply of services, whether temporary or permanent; or
- (ii) a loss of opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;
- (q) “Member” means a Member of the Board and includes the Chairperson;
- (r) “notification” means a notification published in the Official Gazette and the expressions “notify” and “notified” shall be construed accordingly;
- (v) an association of persons or a body of individuals, whether incorporated or not;
- (vii) every artificial juristic person, not falling within any of the preceding sub-clauses;
- (t) “personal data” means any data about an individual who is identifiable by or in relation to such data;
- (u) “personal data breach” means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;
- (v) “prescribed” means prescribed by rules made under this Act;
- (w) “proceeding” means any action taken by the Board under th

[recovered from the vector store — section2.html p.3]

e provisions of this Act;

(x) “processing” in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(y) “she” in relation to an individual includes the reference to such individual irrespective of gender;

(z) “Significant Data Fiduciary” means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10;

(za) “specified purpose” means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder; and

(zb) “State” means the State as defined under article 12 of the Constitution.

← Section 1 DPDPA
Section 3 DPDPA →

DPDPA
Table of contents

Report error

Your message
×

Please keep in mind that this form is only for feedback and suggestions for improvement. Unfortunately, questions will not be answered.

Do not fill this field

0 of 1000 max characters

Submit

Comprehensive Legal Interpretation of Section 2 of the Digital Personal Data Protection Act, 2023

"To define is to limit, but without definition, there is chaos." - Oscar Wilde (adapted)

Section 2 - Definitions

Statutory Text (Partial - Key Definitions)

Section 2. In this Act, unless the context otherwise requires,—

[Note: Section 2 contains 28 definitions from (a) to (za). Below are the most critical ones - full analysis of all 28 definitions follows in this interpretation]

(a) "automated means" means any equipment or software capable of operating automatically in response to instructions given or otherwise for the purpose of processing data;

(j) "Data Fi

[recovered from the vector store — section2.html p.4]

duciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data; (k) "Data Principal" means the individual to whom the personal data relates; (l) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary; (m) "digital personal data" means personal data in digital form; (t) "personal data" means any data about an individual who is identifiable by or in relation to such data; (u) "processing", in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;
[Full definitions continue in interpretation below]

Table of Contents

Executive Summary: The Dictionary of DPDPA

Core Actors: Data Principal, Data Fiduciary, Data Processor

Data Types: Personal Data, Digital Personal Data

Key Operations: Processing, Automated Means

Special Categories: Child, Significant Data Fiduciary, Consent Manager

Rights & Obligations Terms: Consent, Notice, Purpose, Grievance

Institutional: Board, Central Government

Complete Analysis: All 28 Definitions (A to ZA)

1. Executive Summary: The Dictionary of DPDPA

Section 2 is the Rosetta Stone of the DPDPA - it defines 28 key terms that appear throughout the Act.

🔍 Why Definitions Matter

Without Definitions:

"Data Fiduciary must obtain consent from Data Principal before processing personal data"

Question: Who is Data Fiduciary? What is consent? What is processing? What is personal data?

Answer: Chaos. Litigation. Uncertainty.

With Definitions (Section 2):

"Data Fiduciary" = defined in Section 2(j)

"consent" = defined in Section 2(f)

"processing" = defined in Section 2(u)

"persona

[recovered from the vector store — section2.html p.5]

Result: Clarity. Certainty. Enforceability.

Legal Principle: Inclusion of one is exclusion of another. What's IN the definition is covered; what's OUT is not.

1.1 The 28 Definitions - Quick Reference

Letter | Term | One-Line Summary

- (a) | automated means | Equipment/software that processes data automatically
- (b) | Board | Data Protection Board of India
- (c) | Chairperson | Chairperson of the Board
- (d) | child | Individual below 18 years
- (e) | Consent Manager | Entity that enables Data Principal to give/manage/withdraw consent
- (f) | consent | Free, specific, informed, unconditional, unambiguous agreement
- (g) | Data Fiduciary | Entity that determines purpose & means of processing
- (h) | Data Principal | Individual whose personal data is processed
- (i) | Data Processor | Entity that processes data on behalf of Data Fiduciary
- (j) | digital personal data | Personal data in digital form
- (k) | e-governance (not in DPDPA) | -
- (l) | grievance | Complaint regarding rights violations
- (m) | identifier | Information that identifies Data Principal
- (n) | incapacity | Physical/mental condition preventing rights exercise
- (o) | Member | Member of the Board
- (p) | personal data | Data about identifiable individual
- (q) | personal data breach | Unauthorised access/use/disclosure/alteration/destruction
- (r) | prescribed | Prescribed by rules under this Act
- (s) | processing | Any operation on personal data (collection, storage, use, etc.)
- (t) | purpose | Objective for which personal data is processed
- (u) | regulations | Regulations made by Board
- (v) | Significant Data Fiduciary | Data Fiduciary notified by Govt due to volume/sensitivity
- (w) | State | Definition per Article 12 of Constitution
- (x) | verifiable consent | Consent obtained through Consent Manager
- (y) | website | Website as per IT Act 2000
- (z) | word processing application | Software for creating/editing documents
- (za) | year | Year per General Clauses Act

[recovered from the vector store — section2.html p.6]

Section 2(k): "Data Principal means the individual to whom the personal data relates"

🔍 Data Principal Explained

In Simple Terms: YOU (if it's your data being processed)

Key Word: "individual"

🔍 Natural persons (humans)

🔍 NOT companies, organizations, LLPs, trusts, associations

Examples:

Customer whose shopping data is collected by Amazon → Data Principal

Patient whose health records are maintained by hospital → Data Principal

Employee whose HR data is processed by employer → Data Principal

User whose browsing data is tracked by Google → Data Principal

Child whose photos are posted by parent on social media → Data Principal (even though child didn't consent)

Data Principal has RIGHTS:

Right to notice (Section 5)

Right to consent/withdraw consent (Section 6)

Right to access (Section 11)

Right to correction & erasure (Section 12)

Right to grievance redressal (Section 13)

Right to nominate (Section 14)

Data Principal has DUTIES:

Comply with laws (Section 15(a))

No false complaints (Section 15(b))

No impersonation (Section 15(c))

No suppression of legally required info (Section 15(d))

Provide authentic info (Section 15(e))

2.2 Data Fiduciary - Section 2(j)

🔍 DEFINITION

Section 2(j): "Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data"

🔍 Data Fiduciary Explained

In Simple Terms: The organization/person deciding WHY and HOW to process data

Two Key Tests:

Determines PURPOSE: Why are we collecting this data?

Determines MEANS: How will we process it? (What systems, what security, etc.)

If you decide both → You're Data Fiduciary

Word "Fiduciary" is Important:

Fiduciary = Position of trust and confidence

Data Fiduciary holds data IN TRUST for Data Principal

Must act in Data Principal's interests, not just own interests

Examples:

Amazon India → Data Fiduciary (

[recovered from the vector store — section2.html p.7]

decides to collect customer data for order fulfillment)

Hospital → Data Fiduciary (decides to collect patient data for treatment)

Employer → Data Fiduciary (decides to collect employee data for payroll, HR)

Google → Data Fiduciary (decides to collect user data for ads, analytics)

Social Media Platform → Data Fiduciary (decides to collect user content for hosting, showing to others)

"alone or in conjunction with other persons":

Can be:

Sole Fiduciary: One entity decides everything

Joint Fiduciaries: Multiple entities jointly decide (e.g., two banks jointly processing customer data for co-branded credit card)

Data Fiduciary has OBLIGATIONS:

Section 8: Ensure security, notify breaches

Section 9: Extra duties for children's data

Section 10: If Significant Data Fiduciary - more duties

Data Fiduciary is LIABLE:

Section 33: Penalties up to ₹500 crores

Civil liability for damages

2.3 Data Processor - Section 2(l)

🔍 DEFINITION

Section 2(l): "Data Processor means any person who processes personal data on behalf of a Data Fiduciary"

🔍🔍 Data Processor Explained

In Simple Terms: Service provider that processes data following Fiduciary's instructions

Key Phrase: "on behalf of"

Processor doesn't decide WHY or WHAT to do with data

Processor follows Fiduciary's instructions on HOW to process

Examples:

Cloud Service Provider (AWS): Stores customer data on behalf of e-commerce company (Fiduciary) → Processor

Payroll Company: Processes employee salaries on behalf of employer (Fiduciary) → Processor

Call Center (BPO): Handles customer service on behalf of bank (Fiduciary) → Processor

Email Marketing Platform: Sends emails on behalf of retailer (Fiduciary) → Processor

Medical Transcription Service: Transcribes patient notes on behalf of hospital (Fiduciary) → Processor

Processor vs Fiduciary - The Test:

[recovered from the vector store — section2.html p.8]

r | Data Fiduciary

Who decides WHY to collect data? | Fiduciary decides | I decide

Who decides WHAT data to collect? | Fiduciary decides | I decide

Who decides HOW to process? | Fiduciary gives instructions, I follow | I decide

Can I use data for my own purposes? | ☐ NO | ☐ YES (within legal limits)

Who faces penalties under DPDPA? | Not directly (but Fiduciary liable for my violations) | I face penalties

CRITICAL: Processor has NO direct obligations or penalties under DPDPA

BUT Data Fiduciary is responsible for Processor's actions (Section 8(9))

Therefore, Fiduciary must:

Choose processors carefully

Have Data Processing Agreements

Ensure processor has adequate security

Monitor processor compliance

Can Processor become Fiduciary?

☐ YES - if Processor starts using data for OWN purposes beyond Fiduciary's instructions

Example: AWS (normally Processor) decides to analyze customer data stored on its servers for its own AI training → Becomes Fiduciary for that processing

3. Data Types: What's Covered

3.1 Personal Data - Section 2(t)

☐ DEFINITION

Section 2(t): "personal data means any data about an individual who is identifiable by or in relation to such data"

☐ Personal Data Explained

Two Elements Required:

Data about an individual (not about companies)

Individual is identifiable from that data

"Identifiable" is Key:

Can this data be used to identify a specific person (alone or combined with other data)?

☐ Personal Data Examples:

Direct Identifiers: Name, Aadhaar number, PAN, passport number, phone, email

Physical Attributes: Photos, fingerprints, DNA, voice recordings, facial recognition data

Online Identifiers: IP addresses, cookie IDs, device IDs, email addresses, social media handles

Location Data: GPS coordinates, address, check-ins

Financial Data: Bank account numbers, credit card numbers, salary, transaction history

Health Data: Medical records, prescriptions, test results, insurance claims

Behavioral Data: Browsing history, purchase hi

[recovered from the vector store — section2.html p.9]

story, app usage, search queries

Sensitive Attributes: Religion, caste, sexual orientation, political views (if linked to identifiable individual)

❓ NOT Personal Data Examples:

Aggregate statistics: "25% of users are aged 25-35" (no individual identifiable)

Truly anonymized data: Data stripped of all identifiers, cannot be re-identified

Company information: "ABC Corp's revenue is ₹100 crores" (not about individual)

Public information de-linked from individual: "Most popular product is laptops" (no person identified)

❓❓ Borderline Cases:

Pseudonymized Data:

User ID "User123456" with browsing history but no name/email

Answer: STILL personal data if User ID can be linked back to individual (e.g., if company has mapping of User ID to email)

Hashed Email:

Email converted to cryptographic hash: "john@example.com" → "5d41402abc4b2a76b9719d911017c592"

Answer: STILL personal data (hash can be reversed by comparing against email database)

Differential Privacy:

Statistical database with noise added so individual records cannot be inferred

Answer: NOT personal data if properly implemented (truly anonymous)

3.2 Digital Personal Data - Section 2(m)

❓ DEFINITION

Section 2(m): "digital personal data means personal data in digital form"

❓ Digital Personal Data Explained

Digital Form = Electronic/Binary Format

❓ Digital Personal Data Examples:

Data entered on website/app

Emails, text messages

Digital photos, videos

Voice recordings (audio files)

Data stored on computers, servers, cloud

Biometric scans stored digitally

Paper forms SCANNED and stored as PDFs

Handwritten notes TYPED into computer

❓ NOT Digital Personal Data:

Handwritten paper forms (never digitized)

Physical photographs (never scanned)

Verbal conversations (never recorded)

Paper-based medical records (in filing cabinet, never digitized)

Key Point from Section 1(2)(a):

Data collected in NON-DIGITAL form and THEN digitized = Covered by DPDPA

Example:

Patient fills paper form at clini

[recovered from the vector store — section2.html p.10]

Section 2(u): "processing, in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction"

?? Processing Explained

Processing = ALMOST ANYTHING you do with data

Explicitly Mentioned Operations:

Collection: Obtaining data from Data Principal (form fill, app input, cookies)

Recording: Capturing data (writing to database, logging)

Organisation: Arranging data (sorting by name, grouping by category)

Structuring: Giving data a format (database schema, JSON format)

Storage: Keeping data (on servers, cloud, hard drives)

Adaptation: Modifying for different use (converting format, translating)

Alteration: Changing data (updating address, correcting typo)

Retrieval: Accessing stored data (database query, search)

Use: Applying data for purpose (using email to send newsletter, using address to ship product)

Alignment/Combination: Linking datasets (matching email across databases, merging customer profiles)

Indexing: Creating searchable index (search engine indexing web pages)

Disclosure by Transmission: Sending data to third party (emailing data to partner)

Dissemination: Widely sharing data (publishing on website)

Making Available: Providing access (API access, portal for viewing)

Restriction: Limiting processing (archiving, marking for no further use)

Erasure: Deleting data

Destruction: Permanently destroying (shredding, secure deletion)

Word "includes" = Non-Exhaustive List

These are EXAMPLES.

[recovered from the vector store — section2.html p.11]

ons:

Just STORING data = processing

Backup copies = processing

Archiving old data = processing

Key Phrase: "wholly or partly automated"

Must involve some automation (computers, software)

Covered: Fully automated (AI algorithm), Semi-automated (human + computer)

Not Covered: Purely manual (hand-sorting paper files) - but DPDPA only applies to digital data anyway

Complete Analysis: All 28 Definitions (A to ZA)

Below is comprehensive analysis of EVERY definition in Section 2:

(a) "automated means"

Definition: "any equipment or software capable of operating automatically in response to instructions given or otherwise for the purpose of processing data"

Meaning: Technology that processes data without continuous human intervention

Examples:

Computers, servers, smartphones

Software applications (databases, CRM systems, AI algorithms)

Automated systems (chatbots, recommendation engines, fraud detection)

IoT devices processing data (smart speakers, fitness trackers)

Why It Matters: DPDPA applies to processing that is "wholly or partly automated" - this defines what "automated" means

(b) "Board"

Definition: "the Data Protection Board of India established under sub-section (1) of section 18"

Meaning: The regulatory authority for data protection in India

Functions (Section 18-32):

Investigate complaints

Impose penalties

Issue directions

Conduct inquiries

Issue guidance

Monitor compliance

Composition: Chairperson + Members (max 6), appointed by Central Government

Powers: Civil court powers - summon, examine witnesses, require documents, impose penalties up to ₹500

crores

Headquarters: To be notified by Central Government

(c) "Chairperson"

Definition: "the Chairperson of the Board"

Qualifications (Section 19):

Expertise in data protection, information technology, data management, cybersecurity, or other relevant field

Term: 3 years or age 65, whichever earlier (re-appointment possible)

Role: Leads the Board, presides over meetings, administ

[recovered from the vector store — section2.html p.12]

Definition: "an individual who has not completed the age of eighteen years"

Why It Matters: Section 9 provides special protections for children's data:

Prohibits tracking, behavioral monitoring, targeted advertising

Prohibits any processing likely to cause harm to child

Age Determination: How to verify? Rules may specify (Aadhaar, self-declaration with parent verification, age estimation)

Note: Different from "minor" in some other laws (e.g., 21 for some purposes). DPDPA uses 18.

Definition: "any person registered with the Board who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform"

Meaning: Intermediary that helps Data Principals manage their consents across multiple Data Fiduciaries

Think of it as: "Consent Dashboard" or "Privacy Control Center"

Single interface to give consent to multiple services

Interoperable (works with all Data Fiduciaries using consent standard)

Must be Registered with Board: Not anyone can be Consent Manager - must meet Board's standards, register, comply with regulations

Inspiration: Account Aggregators in financial sector (similar concept - single point for managing financial data sharing)

User wants to sign up for 10 different websites. Instead of giving consent separately to each:

User uses Consent Manager (e.g., "DigiLocker Consent" or "MyData Manager")

All 10 websites integrate with Consent Manager

User gives consent once via Consent Manager

Consent Manager communicates with all 10 websites

Later, user can revoke consent to any/all via single dashboard

Status: Framework being developed - Rules w

[recovered from the vector store — section2.html p.13]

ill specify standards, registration process

Definition: "a freely given, specific, informed, unconditional and unambiguous indication of the Data Principal's agreement to the processing of her personal data for a specified purpose"

Freely given: No coercion, pressure, consequences for refusal

Specific: For particular purpose, not blanket consent

Informed: Data Principal knows what they're consenting to

Unconditional: Not bundled with unrelated services

Unambiguous: Clear affirmative action, not silence or pre-ticked boxes

See Section 6 interpretation for full analysis (25,000+ words dedicated to consent)

[Already covered comprehensively in Section 2.2 above]

[Already covered comprehensively in Section 2.1 above]

[Already covered comprehensively in Section 2.3 above]

[Already covered comprehensively in Section 3.2 above]

Definition: "any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data"

Confidentiality Breach: Unauthorized access/disclosure (data leak, hacking)

Integrity Breach: Unauthorized alteration/destruction (data tampering, corruption)

Availability Breach: Loss of access (ransomware, system failure, accidental deletion)

Key Word: "unauthorised" or "accidental"

If intentional AND authorized = not a breach

If unintentional OR unauthorized = breach

Hacker gains access to customer database → Confidentiality breach

Employee accidentally emails customer list to wrong recipient → Confidentiality breach

Ransomware encrypts files, company can't access → Availability breach

Disgruntled employee alters customer records → Integrity breach

[recovered from the vector store — section2.html p.14]

→ Availability breach

Obligation (Section 8(6)): Must notify Board + affected Data Principals within prescribed time (likely 72 hours per Rules)

(v) "Significant Data Fiduciary"

Definition: "any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10"

Meaning: Data Fiduciaries designated by Government as "significant" due to volume of data, sensitivity, or risk

Criteria for Notification (Section 10):

Volume and sensitivity of personal data processed

Risk to rights of Data Principals

Impact on sovereignty and integrity of India

Risk to electoral democracy

Security of the State

Public order

Additional Obligations (Section 10):

Appoint Data Protection Officer (DPO)

Conduct Data Protection Impact Assessment (DPIA)

Undergo periodic Data Protection Audit

Other measures as prescribed

Likely SDFs (Once Notified):

Google, Facebook, Amazon, Microsoft (tech giants)

Large banks, telecom companies

Social media platforms with >10 million Indian users

Healthcare platforms processing sensitive health data

Financial technology companies

See Section 10 interpretation for full analysis (22,000+ words)

Section 2 provides the foundation - without these definitions, the rest of DPDPA would be meaningless.

"Words are the building blocks of law. Define them precisely, and the structure stands firm. Define them poorly, and chaos ensues." - Legal Wisdom

Most Critical Definitions to Remember:

Data Principal (2(k)): Individual whose data it is - has RIGHTS

Data Fiduciary (2(j)): Entity processing data - has OBLIGATIONS & faces PENALTIES

Data Processor (2(l)): Service provider - no direct DPDPA obligations

Personal Data (2(t)): Data about identifiable individual

Processing (2(u)): ANYTHING done with data

Consent (2(f)): FISU-U agreement

Child (2(d)): Under 18 = special protections

Significant Data Fiduciary (2(v)): Big players with extra obligations

Personal Data Breach (2(q

[recovered from the vector store — section2.html p.15]

)): Security incident requiring notification

Board (2(b)): The regulator - investigates, penalizes, guides

Why Definitions Matter in Practice:

Scenario: "Company X processes personal data"

Questions Raised:

Is Company X a Data Fiduciary or Data Processor? → Check 2(j) vs 2(l)

Is it "personal data"? → Check 2(t) - is individual identifiable?

Is it "processing"? → Check 2(u) - yes, any operation counts

Does it need "consent"? → Check 2(f) for what valid consent means

If involving children? → Check 2(d) - under 18?

If breach occurs? → Check 2(q) - confidentiality/integrity/availability compromised?

Each definition is a key that unlocks different parts of DPDPA.

Master Section 2, and you've mastered the language of Indian data protection law.

Comprehensive Legal Interpretation Complete
Section 2 DPDPA 2023 - Definitions

🔍 All 28 definitions analyzed

🔍 Core actors explained (Data Principal, Fiduciary, Processor)

🔍 Data types (Personal, Digital Personal)

🔍 Key operations (Processing, Automated Means)

🔍 Special categories (Child, SDF, Consent Manager)

🔍 50+ practical examples

🔍 Comparison tables

🔍 Identifiable vs anonymous data

🔍 Processor vs Fiduciary test

🔍 Personal data breach types

🔍 Consent Manager framework

© 2026 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert