

The dawn of a new age of privacy in India

The Digital Personal Data Protection Act (DPDPA), 2023 and Rules, 2025



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

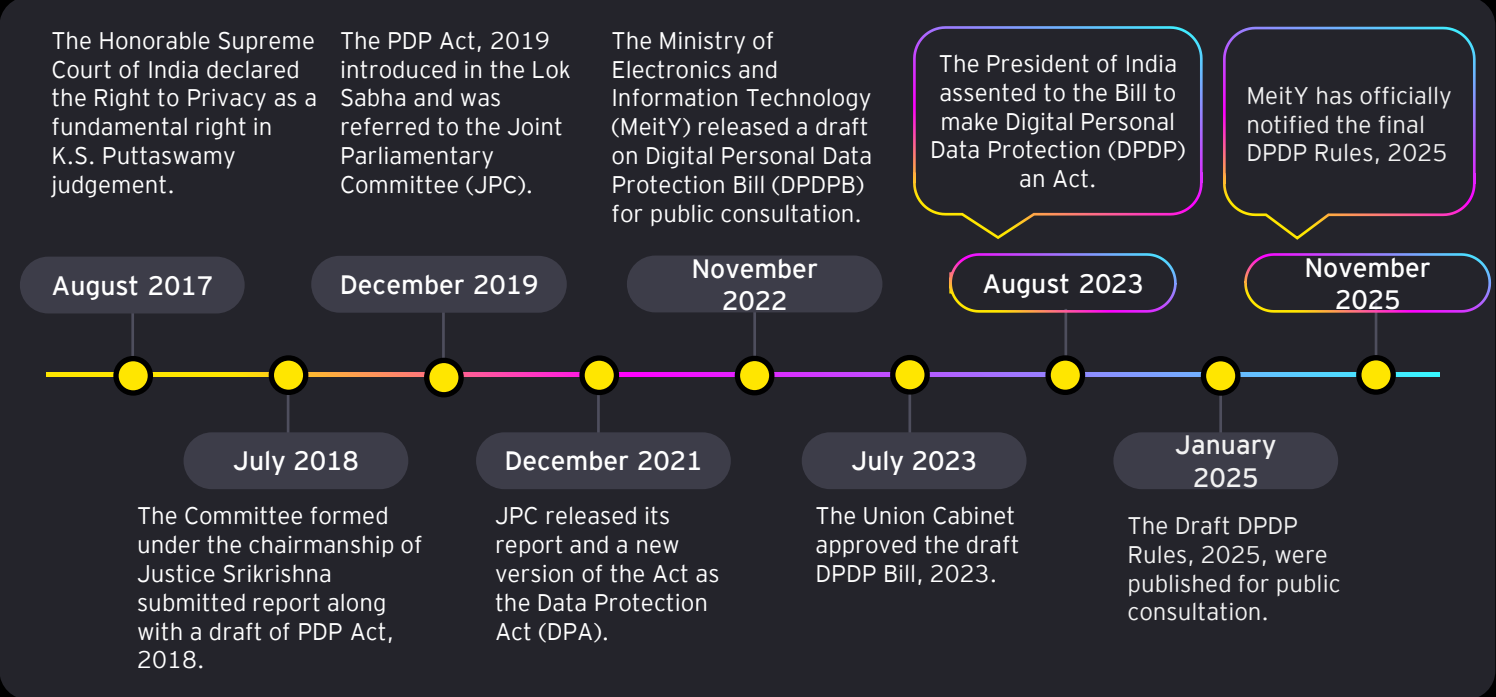


Shape the future
with confidence

Digital Personal Data Protection Act, 2023

Journey so far

Below is the timeline of the DPDPA Act, outlining its release and the key milestones in its implementation.



Applicability of the Act



Processing of digital and digitized personal data

- Processing of personal data within the territory of India and outside of India
- Data that is in digital format or in non-digital form and digitized subsequently
- Activity related to offering goods and services to Data Principals within India



Does not apply to

- Processing for domestic or personal purposes by individuals
- Personal data made publicly available by:
 - Data Principal to whom such personal data relates
 - Any other person who is under an obligation under any law

Exemptions to the Act





- Processing personal data necessary for **research, archiving, or statistical purposes** is exempted, provided it meets the standards specified in Second Schedule of DPDP Rules, 2025
- Certain instrumentalities of the Government of India are exempted from compliance when processing is in the interest of **sovereignty, security, public order, or national integrity**, as notified by the government


Digital Personal Data Protection Act, 2023

Key aspects of the Act

Key definitions

 **Personal data** means any personal data about an individual who is identifiable or in relation to such a person

 **Data Fiduciary** means who alone or in conjunction with other persons determines the purpose and means of processing of Personal Data.

 **Significant Data Fiduciary** any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government on the basis of an assessment of relevant factors.

Notice

Shall be clear, itemized, in plain language and should include

- Purpose of processing
- Manner for accessing rights
- Manner of making a complaint to the board

Notice to be provided in English or to have an option for any language specified in the Eighth Schedule of the Indian Constitution.

Children's data

The Data Fiduciary shall adopt appropriate technical and organizational measures to ensure that verifiable consent of the parent is obtained.

Behavioral monitoring of children or targeted advertising directed at children is prohibited.

Data principal rights

- Rights to access
- Right to correction and erasure
- Rights of grievance redressal
- Right to nominate

Transfer of personal data outside India

Personal data processed by Data Fiduciaries may be transferred outside India, provided that the Data Fiduciaries comply with the conditions or directions issued by the Central Government for such transfers.

Grounds for processing personal data

Consent

Consent from a Data Principal shall be:

- free, specific and informed;
- unconditional and unambiguous with clear affirmative action

Legitimate uses



Data Principal has voluntarily provided her personal data



Performance of any law or in the interest of sovereignty, integrity of India or security



To issue any subsidy, benefit, service, certificate, license or permit



Compliance with any legal judgement, decree or order



Responding to a medical emergency involving a threat to life



With the epidemic outbreak of disease, or any other threat to public health



For safety in the case of any disaster, or any breakdown of public order



For the purpose of employment or those related to safeguarding the employer from loss or liability

Penalties of non-compliance

- Non-compliance of the provisions by Data Fiduciaries up to **INR 250 crore**
- Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards up to **INR 250 crore**
- Breach in observance of duty of Data Principal up to **INR 10,000**
- Breach in not giving notice of personal breach up to **INR 200 crore**
- Breach in observance of additional obligation in relation to children up to **INR 200 crore**
- Breach in observance of additional obligations of Significant Data Fiduciary up to **INR 150 crore**

Digital Personal Data Protection Rules, 2025

Key aspects of the Rules

The DPDP Act, approved by the President of India on **11 August 2023**, is now set for effective implementation following the official notification of the final DPDP Rules by MeitY on **13 November 2025**

23 Rules

14 are directly applicable to the **Data Fiduciary**, while the remaining provisions address the establishment and operation of the **Data Protection Board**, the registration and obligations of the **Consent Manager**, and the standards to be followed while processing personal data by the **State and its instrumentalities**.

Notice and Consent

Data Fiduciaries shall:

- Provide notices in **clear** and **plain** language with :
 - Itemised Description** of the personal data
 - Specified purpose** for processing of personal data.
- Provide communication link to Data Principals through website/app

Consent manager

Consent Manager shall:

- Be Registered with the Board and meet all eligibility requirements according to the **Part A of First Schedule**.
- Manage consent flows securely and maintain detailed consent records for at least **7 years**, or longer if required by law or agreed with the Data Principal

Reasonable Security safeguards

Data Fiduciaries shall:

- Implement strong reasonable security safeguards such as encryption, masking, obfuscation, access controls, activity logging, backups and business continuity
- Maintain visibility through monitoring, reviews and **one year log retention**.

Personal data breach

Data Fiduciaries shall:

- Notify affected Data Principals and the Board **without any delay** after discovering a personal data breach.
- Submit a report with updated and detailed information related to the breach to the Board within **72 hours** of becoming aware of the breach.

Data retention timelines

Data Fiduciaries shall:

- Define clear data erasure timelines specific to the purpose of processing personal data
- Retain logs including traffic related to data processing transactions for a **minimum of one year**.
- Notify the Data Principal at least **48 hours** before erasing their personal data once the purpose is fulfilled or no longer applies.

Data principal rights

Data Fiduciaries shall:

- Publish clear channels and means for Data Principals to submit rights requests on their websites/apps or both.
- Maintain a data principal grievance system that responds to issues within **90 days**.

Verifiable Parental Consent

Data Fiduciaries shall:

- Obtain **verifiable parental consent** before processing any child's personal data.
- Use reliable identity and age verification methods (ID details or authorised digital tokens).
- Implement technical measures to ensure verifiable consent is obtained from parent of a child


Exception to Verifiable Parental Consent

Obligations on processing of children's personal data shall not be applicable to a Data Fiduciary who:

- Is a **health professional or an allied healthcare professional**.
- Is an **educational institution and/or creche**.
- Is a **child transport provider** and tracks location during travel for safety

Digital Personal Data Protection Rules, 2025


Key aspects of the Rules



Significant Data Fiduciary (SDF)

Significant Data Fiduciaries shall:


- Conduct **Data Protection Impact Assessments (DPIA)** and **audits annually**
- Cause the person carrying out DPIA and audit to furnish to the Board a report containing **significant observations**
- Ensure due diligence in technical measures including **algorithmic software's**



Verifiable Consent (Person with Disability)


Data Fiduciaries shall:

- Obtain **verifiable consent** from the lawful guardian
- Verify identity of the lawful guardian and verify that the lawful guardian is appointed by a court, designated authority, or local level committee as per applicable guardianship laws



Data Protection Board of India

- The Data Protection Board of India is the regulatory body responsible for monitoring compliance with the DPDP Act and Rules
- Based in the National Capital Region (NCR), it operates as a fully digital office
- The Board will be constituted by a **Search-cum-Selection Committee** headed by the **Cabinet Secretary**



Deletion of Personal Data


Data Fiduciaries in the following classes must retain personal data for only **three years** from the last time the Data Principal approached them:


- E-commerce entities** with at least 2 crore registered users in India
- Online gaming intermediaries** with at least 50 lakh registered users in India
- Social media intermediaries** with at least 2 crore registered users in India


07


Schedules


3 Schedules outline requirements to guide Data Fiduciaries in taking appropriate actions to achieve compliance, while the remaining Schedules pertain to the operation of the Board and the processing of personal data by the State and its instrumentalities


- 


First Schedule: Defines eligibility and operational obligations for Consent Managers.
- 

Second Schedule: Specifies the standards for processing of personal data by the State and its instrumentalities.
- 

Third Schedule: Specifies retention timelines pertaining to each class of Data Fiduciary.
- 

Fourth Schedule: Identifies eligible Class of Data Fiduciaries and purposes that are exempted from the conditions of processing children's data.
- 

Fifth Schedule: Details the terms and conditions of service for the Chairperson and other members of the Data Protection Board.
- 

Sixth Schedule: Provides the terms and conditions of appointment and service for officers and employees of the Data Protection Board.
- 

Seventh Schedule: Describes the purpose under which the central government may require the Data Fiduciary or the intermediaries to furnish information as requested.

Digital Personal Data Protection Rules, 2025

Timeline for implementation

Below is the implementation timeline for the rules that all Data Fiduciaries must adopt in order to ensure compliance and safeguard the personal data of Data Principals.

Now

Rules 1, 2 and 17 to 21 shall come into effect **immediately on the date of their publication** in the Official Gazette.

- **Rule 1:** Provides the title of the Rules and specifies the date from which the Rules shall come into force
- **Rule 2:** Defines essential terms used throughout the Rules
- **Rule 17:** Provide details on appointment of Chairperson and other member for Data Protection Board of India (Board)
- **Rule 18:** Provide details on salary, allowances, and other terms and conditions of service of Chairperson and other Members of the Board
- **Rule 19:** Defines procedure for meetings of Board and authentication of its orders, directions and instruments.
- **Rule 20:** Provide details on functioning of Board as digital office.
- **Rule 21:** Defines terms and conditions of appointment and services of officers and employees of Board.

12 Months

~ November 2026

Rule 4 shall come into force **one year after the date of publication** of the Gazette

- Rule 4: Provides details on registration and obligations of the Consent Manager

18 Months

~May 2027

Rules 3, 5 to 16, 22 and 23 shall come into force **eighteen months** after the date of publication of the Gazette.

- **Rule 3:** Provide details on the content of the notice that the Data Fiduciary must provide to the Data Principal when processing their personal data.
- **Rule 5:** Describes that the State and its instrumentalities for subsidies, benefits, licenses, etc process personal data following the standards in the Second Schedule of DPDP Rules 2025.
- **Rule 6:** Describes reasonable security safeguards that Data Fiduciary must implement to safeguard personal data processed by them.
- **Rule 7:** Provide details on intimation of personal data breach to data principals and the Board.
- **Rule 8:** Provide details on the retention timeline to be followed by the Data Fiduciary and the class of Data Fiduciary once the purpose has been fulfilled.
- **Rule 9:** Describes the requirement to publish contact information of a person who can answer questions about data processing on the application or website.
- **Rule 10:** Provide details on the collection of verifiable consent for processing the personal data of a *child.
- **Rule 11:** Provide details on the collection of verifiable consent for processing of personal data of person with disability who has lawful guardian.
- **Rule 12:** Describes exemptions from certain obligations applicable to processing of personal data of child.
- **Rule 13:** Describes additional obligations applicable to Significant Data Fiduciary (SDF).
- **Rule 14:** Provide details on rights of data principal.
- **Rule 15:** Provide details on transfer of personal data outside the territory of India
- **Rule 16:** Describes exemptions from Act for research, archiving or statistical purposes
- **Rule 22:** Provide details on how to appeal to the Appellate Tribunal
- **Rule 23:** Provide details on purposes where Central Government may require the Data Fiduciary or the intermediaries to furnish information as requested.

**Child shall mean any individual who has not completed the age of eighteen years*

Digital Personal Data Protection Rules, 2025

Journey to compliance

As organizations embark on the journey towards compliance with the DPDP Act, 2023 and DPDP Rules 2025 there are multiple facets and requirements as per the Act and could be phased in 0 to 18 months for an effective and sustainable data privacy and protection program.

Now 0 - 6 months

- Develop the data privacy framework to strengthen your organization's data privacy program
- Develop/Refresh privacy notice to clearly articulate the requirements as following:
 - The categories of personal data being collected
 - The purposes for which each data element is captured
 - The mechanisms for data principles to withdraw consent
 - The process through which users can raise concerns or submit grievances
- Conduct data mapping exercise to identify
 - The categories and attributes of personal data captured across the organization
 - Systems, repositories, and environments where this data is stored or processed
 - The internal recipients and external recipients (third parties) with authorized access
 - Flow of data across internal processes and external partners, including all third party vendors
- Enhance/implement baseline security measures such as but not limited to
 - Protection of personal data in transit and at rest
 - Role-based access controls supported by continuous log monitoring
 - Maintenance of audit logs for a minimum of one year
 - Robust backup, disaster recovery, and business continuity protocols
 - Appropriate provision in the contract within all third-party contracts
- Update/develop and operationalized breach response procedure to ensure readiness to notify data principals and Data Protection Board without undue delay
- Establish/Enhance data privacy training program to ensure compliance with the requirements of DPDPA 2023 and Rules 2025
- Define and document data retention procedure to:
 - Establish a mechanism to retain personal data and transactional logs for a period of at least one year
 - Establish a three-year data retention schedule and provide users with at least 48 hours' advance notice prior to any planned deletion for the special classes of Data Fiduciaries

Next 6 - 12 months

- *Establish mechanisms for:
 - Annual Data Protection Impact Assessments (DPIAs)
 - Independent Annual Audits
 - Algorithmic Transparency and Fairness Assessments
 - Potential Data Localisation Requirements

Beyond 12 - 18 months

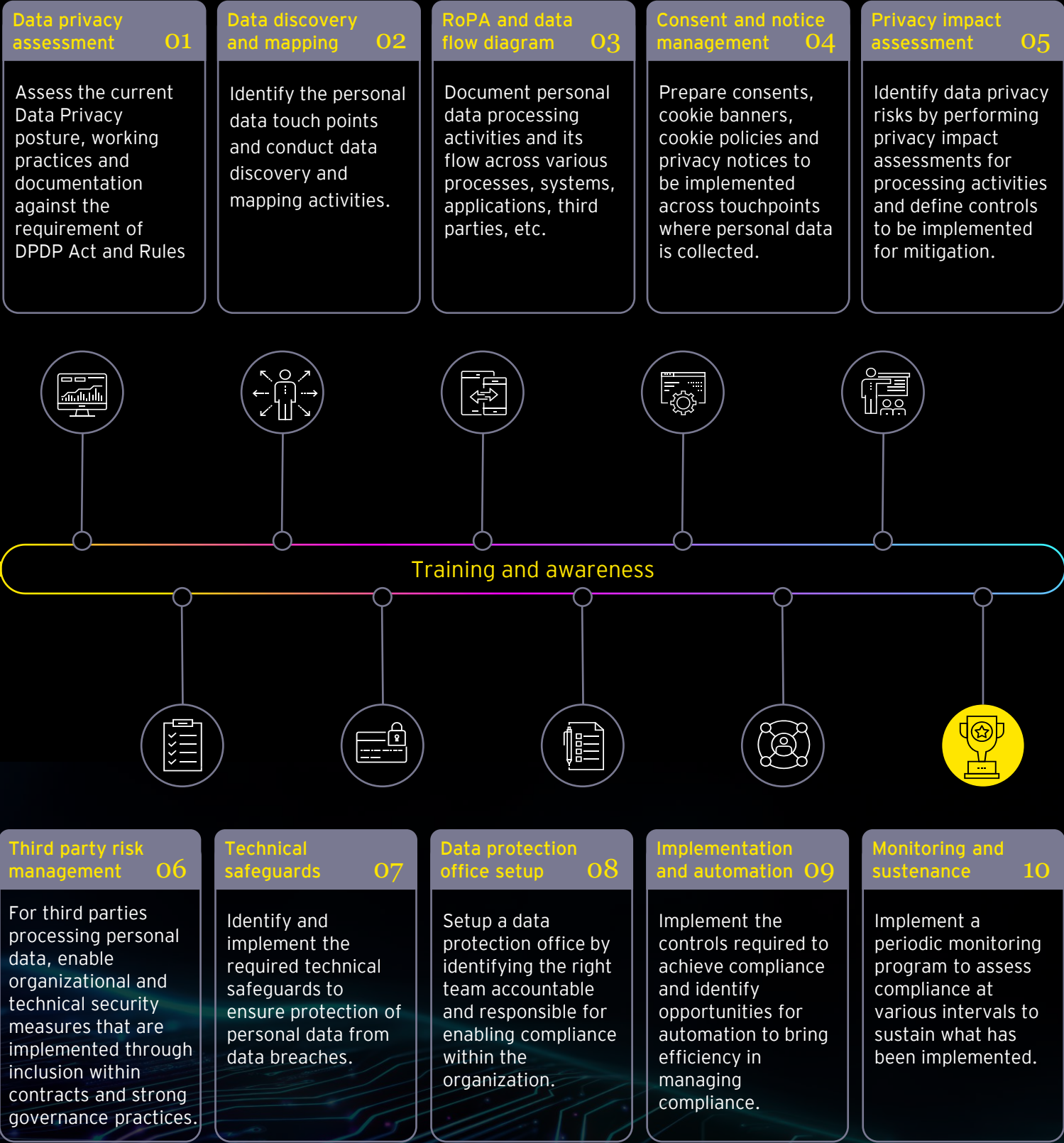
- Implement Privacy Enabling Technologies (PETs) to reduce manual tasks and manage your data governance activities in an automated manner
- Undertake external certifications to demonstrate compliance with the Privacy Information Management System (PIMS)

Note: This timeline is indicative in nature and the associated activities and timeframes may vary depending on the organization's data privacy posture

How can EY help?

Journey to compliance

Our comprehensive transformation strategy takes into account the essential aspects of the Act throughout the organization's data management lifecycle.



Our Offices

Ahmedabad

22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind
Iskcon Temple
Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International
Financial Centre
GIFT City SEZ
Gandhinagar - 382355,
Gujarat
Tel +91 79 6608 3800

Bengaluru

12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560
048
Tel: + 91 80 6727 5000

Bhubaneswar

8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha - 751024
Tel: + 91 674 274 4490

Chandigarh

Elante offices, Unit No. B-
613 & 614
6th Floor, Plot No- 178-
178A
Industrial & Business Park,
Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai

6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv
Gandhi Salai
Taramani, Chennai - 600
113
Tel: + 91 44 6654 8100

Delhi NCR

Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122
003
Haryana
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-
1
IGI Airport Hospitality
District
Aerocity, New Delhi - 110
037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad

THE SKYVIEW 10
18th Floor, "SOUTH
LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur

9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

Kochi

9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata

22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: +91 33 6615 3400

6th floor, Sector V,
Building Omega, Bengal
Intelligent Park, Salt Lake
Electronics Complex,
Bidhan Nagar
Kolkata - 700 091
Tel: +91 33 6615 3400

Mumbai

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400
028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express
Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No 301
Building No. 1
Mindspace Airoli West
(Gigaplex)
Located at Plot No. IT-5
MIDC Knowledge Corridor
Airoli (West)
Navi Mumbai - 400708
Tel: + 91 22 6192 0003

Altimus, 18th Floor
Pandurang Budhkar Marg
Worli, Mumbai - 400 018
Tel: +91 22 6192 0503

Pune

C-401, 4th Floor
Panchshil Tech Park,
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club
Road
Baner, Pune - 411 045
Tel: + 91 20 4912 6800



Contacts

Consulting Services



Murali Rao
Partner and Leader,
Cybersecurity
Consulting, EY India
Murali.Rao@in.ey.com



Raghavendra Bv
Partner and Deputy
Cybersecurity Consulting
Leader, EY India
raghavendra.bv@in.ey.com



Mini Gupta
National Data Privacy
Consulting Partner,
EY India
mini.gupta@in.ey.com



Lalit Kalra
National Data Privacy
Consulting Partner,
EY India
lalit.kalra@in.ey.com



Sujay Maskara
Data Privacy
Consulting Partner,
EY India
sujay.maskara@in.ey.com



Kartik Shinde
Partner, Cybersecurity
Consulting, EY India
kartik.shinde@in.ey.com

Tax & Regulatory Services



Rajiv Chugh
Partner and National
Leader, Policy Advisory and
Specialty Services, EY India
rajiv.chugh@in.ey.com



Ritika Loganey Gupta
Partner - Policy Advisory &
Speciality Services, EY India
ritika.gupta@in.ey.com



Pankaj Sharma
Partner
Telecom - Regulatory
Services, EY India
pankaj.sharma4@in.ey.com

Notes

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, Haryana - 122 003, India.

© 2025 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN2510-026
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RS2

ey.com/en_in