

Digital Personal Data Protection Bill, 2023



Nangia Andersen LLP

A member firm of **ANDERSENGLOBAL**



Foreword



Marking a significant leap towards fortifying individual privacy in the digital era, the Digital Personal Data Protection Bill (DPDP) received the green light from the Lok Sabha (lower house of the Indian Parliament) on August 7, 2023. The Digital Personal Data Protection Bill - a pivotal development shaping India's digital landscape, is poised to become a cornerstone of India's digital governance framework. The bill outlines protocols governing the acquisition and utilization of personal data from Indian citizens, both by corporations and the government. This bill signifies a monumental step in our nation's journey towards robust data protection and privacy. At its core, the bill is anchored in seven fundamental principles, ensuring that the use of personal data is consented, lawful, transparent, and secure. It emphasizes the importance of purpose limitation, data accuracy, minimalistic data usage, limited storage duration, and enforces rigorous security safeguards. The bill reiterates the importance of accountability in the digital age.

At the heart of this bill lies its wide applicability, covering all facets of digital personal data processing within our borders and even extending its grasp to data processed outside, if it pertains to our nation's interests. However, the bill also demonstrates wisdom by introducing thoughtful exemptions, ensuring a balanced approach to data protection.

The introduction of roles such as data processors and fiduciaries, coupled with the rights and duties of data principals, showcases the bill's holistic approach. It not only mandates organizations to bear the onus of data protection but also empowers individuals, ensuring they remain at the center of this data-centric ecosystem.

I believe this bill provides an exciting canvas for businesses to operate within, emphasizing trust, transparency, and responsibility. Navigating the intricacies of this Bill will undoubtedly pose challenges, but it is my firm belief that challenges breed innovation. By embracing the tenets of this bills, we can drive a culture of ethical data handling that not only safeguards our customers' trust but also fuels our growth in a digital age. It reinforces the notion that in the digital age, while data drives decisions, it is trust that fuels sustainable growth.



Rakesh Nangia
Chairman, Nangia Andersen LLP

Digital Personal Data Protection Bill, 2023



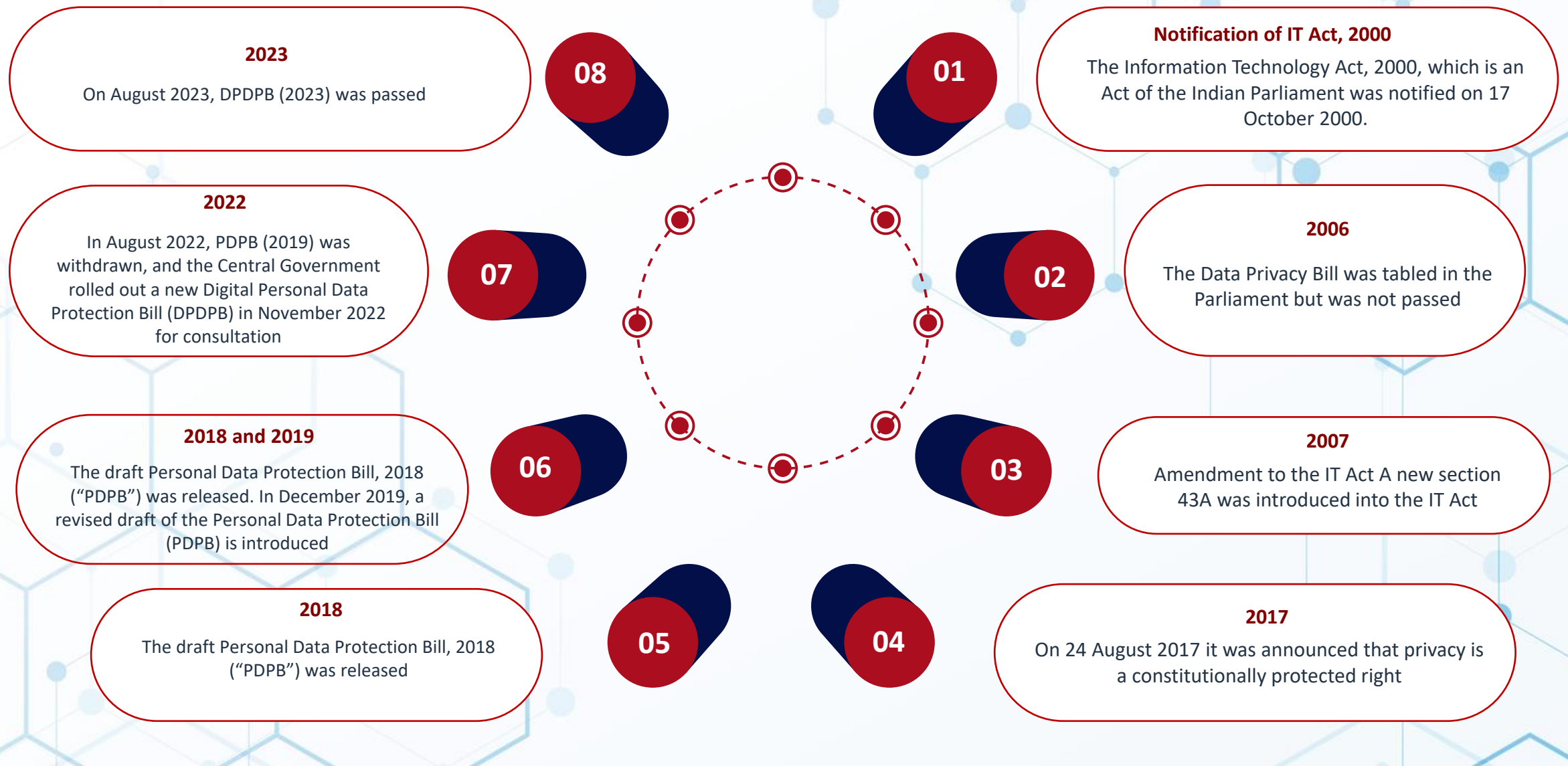
The Digital Personal Data Protection Bill, 2023, aims to ensure the privacy and security of personal data in the digital realm, with provisions governing consent, rights of individuals, obligations of data fiduciaries, and the establishment of a regulatory body for oversight and enforcement.

Personal data is defined as any information that can identify an individual.

The 7 main principles of the bill are:

- The principal of consented, lawful and transparent use of personal data
- The principal of purpose limitation
- The principal of data minimization
- The principal of data accuracy
- The principal of storage limitation
- The principal of reasonable security safeguards
- The principal of accountable





The provisions of this bill would come into effect in six to ten months

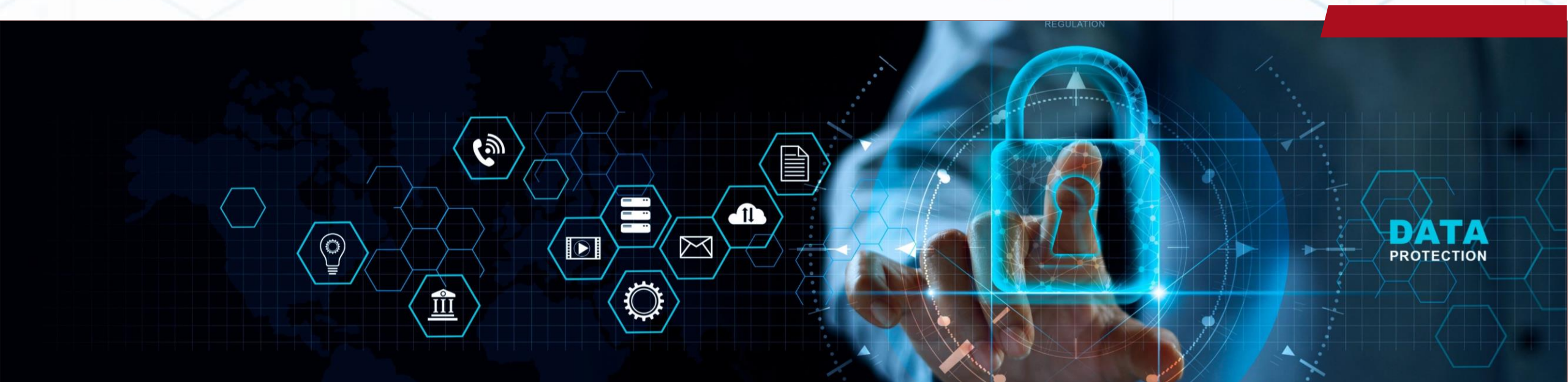


Applicability of this Bill

The Bill is applicable to all collection and processing of digital personal data within India. This includes data collected online or offline, which is then digitized. It also extends to the processing of personal data outside India if it involves offering goods or services within the country. Processing encompasses various operations on this data, such as collection, storage, use, and sharing.

Exemptions to the applicability of the Bill

Non – automated processing of personal data, Offline (non digitized) personal data, Personal data processed by an individual for any personal or domestic purpose, Personal data that has been in existence and on records for at least 100 years



Data processor is anyone who processes personal data on behalf of a data fiduciary

Data fiduciary is anyone who determines the purpose and means of processing of personal data

Obligations of Data Fiduciaries

Data fiduciaries, the entities determining data processing purposes, must ensure data accuracy, implement security safeguards to prevent breaches, notify the Data Protection Board of India and affected parties in case of breaches, and erase data when its purpose is fulfilled, and retention is not legally required.

Significant Data Fiduciaries: Some data fiduciaries can be designated as significant, based on factors like data volume, sensitivity, risks to rights, security considerations, and public order. These entities have extra responsibilities, including appointing data protection officers and conducting impact assessments and compliance audits

Data principal is the natural person whose personal data is processed by a data fiduciary

Rights and Duties of Data Principal

Individuals (data principals) whose data is being processed have several rights, including obtaining information about data processing, requesting data correction and erasure, nominating representatives in case of incapacity, and accessing grievance redressal mechanisms. Data principals also have duties, including not making false complaints or providing misleading information. Failure to adhere to these duties can lead to penalties of up to Rs 10,000.



"The Digital Personal Data Protection bill marks a quantum leap for India's digital realm. Crucially, the bill underscores accountability, transparency, and consent as paramount in the digital data realm like never before. It reinforces the notion that in the digital age, while data drives decisions, it is trust that fuels sustainable growth."

Shrikrishna Dikshit

Partner

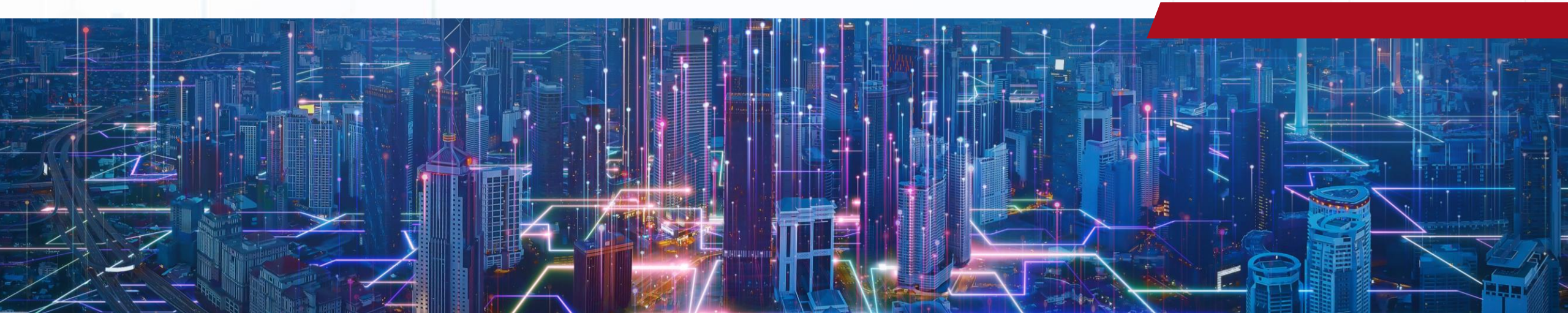
Cyber Security

Consent

Consent of the Data Principal means that any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose. Processing of personal data is permissible only for lawful purposes and after obtaining the consent of the individual. Consent must be preceded by a clear notice that specifies the data to be collected and the intended processing purpose. Consent can be withdrawn at any time. Certain instances, known as 'legitimate uses,' do not require consent, such as situations where data is provided voluntarily, government service provision, medical emergencies, and employment. For individuals under 18, parental or legal guardian consent is necessary.

Data Protection Board of India

The central government will establish the Data Protection Board of India, responsible for monitoring compliance, imposing penalties, directing data fiduciaries during breaches, and addressing grievances



Transfer of Personal Data Outside India

The Bill permits transferring personal data outside India, except to countries restricted by government notifications

Child Data Protection

The Bill requires all data fiduciaries to obtain verifiable consent from the legal guardian before processing the personal data of a child. Additionally, while processing a child's data, data fiduciaries must avoid activities that might harm the child's well – being and must not engage in tracking, behavioral monitoring, or targeted advertising.

Benefits

- Strengthened Privacy Rights
- Protection against Data Breaches and Cyber Threats
- Transparency and Accountability
- Safeguarding Sensitive Personal Information
- Cross Border Data Transfers
- Promoting Ethical Data Practices
- Harmonizing with Global Standards



Penalties for Non Compliance



- **Penalty for Failure to protect a data breach** – Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach – INR 250 Crore.
- **Notification to Board and Data Principals** – Failure to notify the Board and Data Principals in case of a data breach – INR 200 crore
- **Children's data** - Non-fulfilment of obligations while processing children's data - INR 200 crore
- **Significant Data Fiduciary** - Non-fulfilment of obligations when the government notifies a Significant Data Fiduciary - INR 150 crore
- **Non - Compliance of duties of Data Principal** – INR 10,000
- **Miscellaneous** - Non-compliance with provisions of this Act other than those listed in (1) to (5) - Penalty up to INR 50 crore



Exemptions



General Exemptions

Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases.

These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of the Bill. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.

Special Exemptions

Central Government may exempt certain Data Fiduciaries or class of Data Fiduciaries from the below mentioned obligations, basis the volume and nature of personal data processed:

Notice; Data Accuracy, Retention and Disposal; Processing of Children's Personal Data; Additional obligation of Significant Data Fiduciary; Right to information about personal data

Exemptions for Central Government and state

Central government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:

By the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign states, and public order

Necessary for research , archival and statistical reasons where no decision will be taken specific to the data principal

The exempted obligation that shall not apply is Data Retention and Disposal

Meet Our Experts



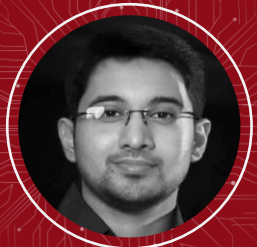
Shrikrishna Dikshit
Partner
Cyber Security



Pushpendra Bharambe
Director
Cyber Security



Aditya Thontakudi
Associate Director
Cyber Security



Karan Pandya
Associate Director
Cyber Security

Our Offices

NOIDA

(Delhi NCR - Corporate Office)
A-109, Sector 136,
Noida – 201304, India
T: +91 120 2598010

DELHI

(Registered Office)
B-27, Soami Nagar,
New Delhi-110017, India
T: +91 120 2598010

GURUGRAM

001-005, Emaar Digital Greens
Tower-A 10th Floor, Golf Course
Extension Road, Sector 61,
Gurgaon-122102, India
T: +0124-4301551/1552

MUMBAI

4th Floor, Iconic Tower, URMI Estate,
Ganpat Rao Kadam Marg, Lower
Parel- 400013, India
T: +91 22 61737000

BENGALURU

Prestige Obelisk, Level 4, No 3
Kasturba Road Bengaluru – 560
001, Karnataka, India
+ 91 80 2248 4555

PUNE

3rd Floor, Park Plaza,
CTS 1085, Ganeshkhind Road,
Next to Pune Central Mall,
Shivajinagar, Pune - 411005, India

CHENNAI

Prestige Palladium Bayan, Level 5,
129-140, Greams Road, Thousand
Lights, Chennai - 600006, India
T: + 91 44 4654 9201

DEHRADUN

First Floor, "IDA" 46 E. C. Road,
Dehradun - 248001,
Uttarakhand, India
T: +91 135 271 6300/301/302/303

