Cybernara

Chirag Goswami

DPDP ACT

The Digital Personal Data Protection Act (DPDPA)

What You Need To Know

Contents:

Cybernara

1. OVERVIEW

Chirag Goswami

The Digital Personal Data Protection Act (DPDPA) was enacted in **August 2023** by the **Indian government**. It is a law designed to ensure that businesses and organizations handle **personal data** responsibly and transparently.

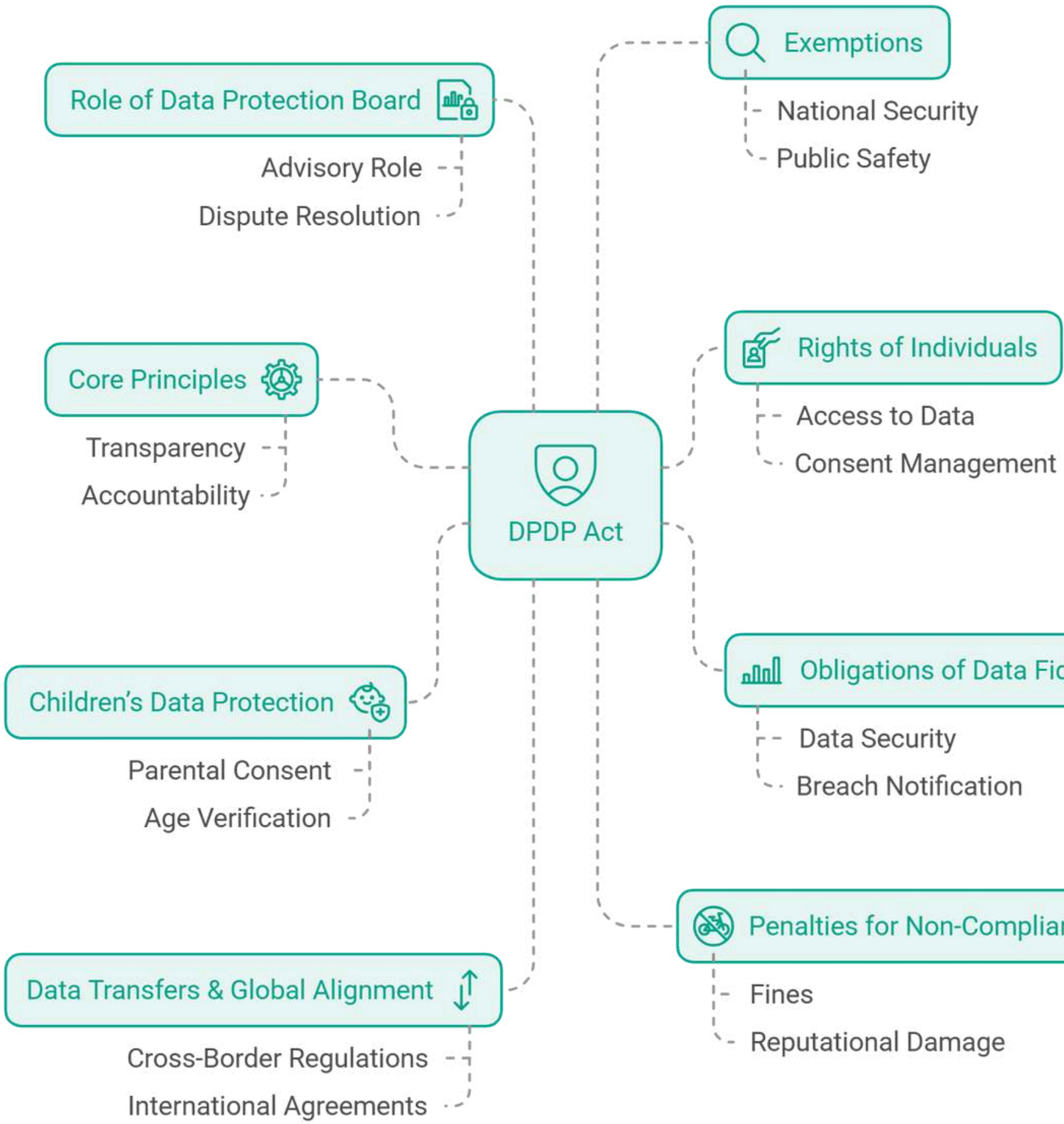
DPDPA requires companies to get clear permission from individuals **before** collecting or using their data and gives people the right to **know, access, or delete** the data collected about them.

The act applies solely to digitally processed personal data for companies operating only in INDIA.

Cybernara

2. DEEPER DIVE

Chirag Goswami



Chirag Goswami

CORE PRINCIPLES

The DPDPA is built on 7 guiding principles:

- **Lawful Use**: Data must be processed only for lawful purposes.
- **Transparency**: Individuals must know how and why their data is being used.
- **Minimization**: Only necessary data should be collected.
- **Data Accuracy**: Organizations must ensure collected data remains accurate and up to date.
- **Storage Limitation**: Data should not be retained longer than required.
- **Security**: Appropriate measures must be in place to protect personal data.
- **Accountability**: Entities processing data must be accountable for their practices.

Chirag Goswami

RIGHTS OF INDIVIDUALS

- Right to **Access**: Know what data is collected and how it is processed.
- Right to **Correction**: Rectify incorrect or incomplete data.
- Right to **Erasure**: Request deletion of outdated or unnecessary data.
- Right to **Grievance Redressal**: Seek help from the Data Protection Board for violations.

OBLIGATIONS OF DATA FIDUCIARIES

- **Purpose Limitation**: Collect data for clearly defined purposes only.
- **Consent Management**: Obtain clear and explicit consent from individuals.
- **Security Safeguards**: Implement robust systems to prevent breaches.
- **Breach Notification**: Inform the Data Protection Board and affected individuals of breaches.

Chirag Goswami

CHILDREN'S DATA PROTECTION

SPECIAL PROVISIONS PROTECT MINORS (UNDER 18 YEARS):

- **Parental Consent**: Mandatory for processing children's data.
- **Prohibited Activities**: No targeted advertising or harmful profiling based on children's data

DATA TRANSFERS & GLOBAL ALIGNMENT

- The act **permits cross-border transfers** of personal data to "trusted" nations notified by the Indian government.
- It aligns India's framework with global standards like the **GDPR**, fostering international trade and collaboration.

Chirag Goswami

PENALTIES FOR NON-COMPLIANCE

- Up to **₹250 crores** for severe violations like failure to prevent breaches.
- The fine system **gradated.** (Gradated is a penalty system where the fine amount depends on the severity or nature of the violation.)

ROLE OF DATA PROTECTION BOARD

THE DATA PROTECTION BOARD OF INDIA IS THE REGULATORY AUTHORITY UNDER DPDPA.

- **Grievance Redressal**: Resolves complaints from individuals.
- **Oversight**: Monitors compliance and imposes fines.

EXEMPTIONS

- **Government Functions**: For national security, public order, or emergencies.
- **Research**: For educational and statistical purposes with safeguards.
- **Legitimate Interests**: To balance public good with privacy rights.

Cybernara

3. How is DPDPA different from Other Acts

Chirag Goswami

Aspect	India (DPDPA)	European Union (GDPR)	United States (CCPA)	United Kingdom (UK GDPR)
Year of Enactment	2023	2018	2020	2018
Scope	Digital-only data	Both digital and physical data	Personal information of California residents	Both digital and physical data
Cross-Border Data Transfers	Allowed to trusted countries only	Allowed to countries with adequate safeguards	Allowed with specific contractual agreements	Allowed to countries with adequate safeguards
Consent Requirement	Explicit and revocable	Explicit, freely given, specific, informed	Implied in some cases; opt-out available	Explicit, freely given, specific, informed
Children's Data Protection	Parental consent for individuals under 18	Parental consent for individuals under 16	Parental consent for individuals under 13	Parental consent for individuals under 16
Rights of Individuals	Access, correction, erasure	Access, correction, erasure, portability	Access, deletion, opt-out from data sale	Access, correction, erasure, portability
Penalties for Non-Compliance	Up to ₹250 crores	Up to €20 million or 4% of global turnover	Up to $7,500 per intentional violation	Up to €20 million or 4% of global turnover
Data Protection Authority	Data Protection Board of India	Independent supervisory authorities in each country	No federal authority; enforced by state-level entities	Information Commissioner's Office (ICO)
Applicability	Organizations processing personal data in India	Organizations processing data of EU residents	Organizations targeting California residents	Organizations processing data of UK residents

Cybernara

4. Common FAQs For Businesses

Chirag Goswami

What do I need to do to comply with the DPDPA?

- Obtain explicit consent from individuals for data collection.
- Implement robust data security measures to protect personal data.
- Have a clear data retention policy and delete data when no longer needed.
- Ensure transparency in how personal data is used and inform individuals of their rights.
- Report data breaches within 72 hours if personal data is compromised.

What should I do if my business experiences a data breach?

You must notify the Data Protection Board of India and the affected individuals within 72 hours of discovering the breach. A breach could lead to penalties, so it's crucial to have a plan for incident response.

Can I transfer personal data to other countries?

- Yes, you can transfer personal data to countries with adequate safeguards (i.e., those providing similar levels of protection as the DPDPA).
- For other countries, you need to implement mechanisms like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

Does the DPDPA apply to my business if I operate outside India?

Yes, the DPDPA applies to all businesses, regardless of location, if they process the personal data of Indian residents. If you handle the data of Indian customers, you must comply with the Act.

How do I obtain consent from individuals under the DPDPA?

Consent must be explicit, informed, and voluntary. You need to clearly inform individuals about what data is being collected and how it will be used. Consent should be easy to withdraw at any time. You can obtain consent through clear checkboxes or written agreements.

What types of personal data are covered under the DPDPA?

The DPDPA covers personal data (e.g., name, contact details, location) and sensitive personal data (e.g., financial data, health data, biometric data) that your business collects, stores, or processes.

What are the penalties for non-compliance with the DPDPA?

Non-compliance can result in penalties up to ₹250 crores for serious violations such as mishandling personal data or failing to report data breaches.

Cybernara

4. Common FAQs For Businesses

Chirag Goswami

How can I ensure my business complies with the DPDPA?

- Regularly train staff on data privacy practices.
- Appoint a Data Protection Officer (if necessary).
- Perform regular audits to ensure data security and compliance.
- Implement clear data protection policies and procedures for data handling.

Does my business need to appoint a Data Protection Officer (DPO)?

Under the DPDPA, a Data Protection Officer (DPO) is required for businesses that process large volumes of personal data or handle sensitive data on a regular basis. The DPO is responsible for ensuring compliance with data protection laws and overseeing data privacy practices.

Can I use personal data for marketing purposes under DPDPA?

- Yes, but only if you obtain explicit consent for marketing purposes. You must also offer an easy way for individuals to opt-out or withdraw consent at any time.
- Data cannot be used for marketing beyond this scope.

Do I need to update my privacy policy?

Yes, your privacy policy must be updated to reflect the requirements of the DPDPA. It should clearly state how you collect, use, and store personal data, as well as individuals' rights under the law.

Does the DPDPA allow businesses to process sensitive data?

Yes, businesses can process sensitive personal data but only under strict conditions, such as obtaining explicit consent from the individual or when required for specific purposes (e.g., medical treatment, legal obligations).

Can I store personal data indefinitely?

No, personal data should only be stored for as long as necessary to fulfill the purpose for which it was collected. Once the data is no longer needed, it must be securely deleted.

Does the DPDPA apply to third-party vendors and partners?

Yes, if third-party vendors or partners process personal data on your behalf, you must ensure they comply with the DPDPA. This can be done through contracts specifying data protection obligations.

Cybernara

5. Conclusion

Chirag Goswami

In conclusion, adhering to the **Digital Personal Data Protection Act** (DPDPA) is not just a legal obligation for businesses, but a crucial step toward building a **cyber-secure environment**.

By implementing the necessary measures to protect personal data, businesses not only safeguard their operations against legal penalties and reputational risks but also foster **trust** and **loyalty** among their customers.

Compliance with the DPDPA is an investment in your business's long-term sustainability creating a solid foundation for future growth in a data-driven world.