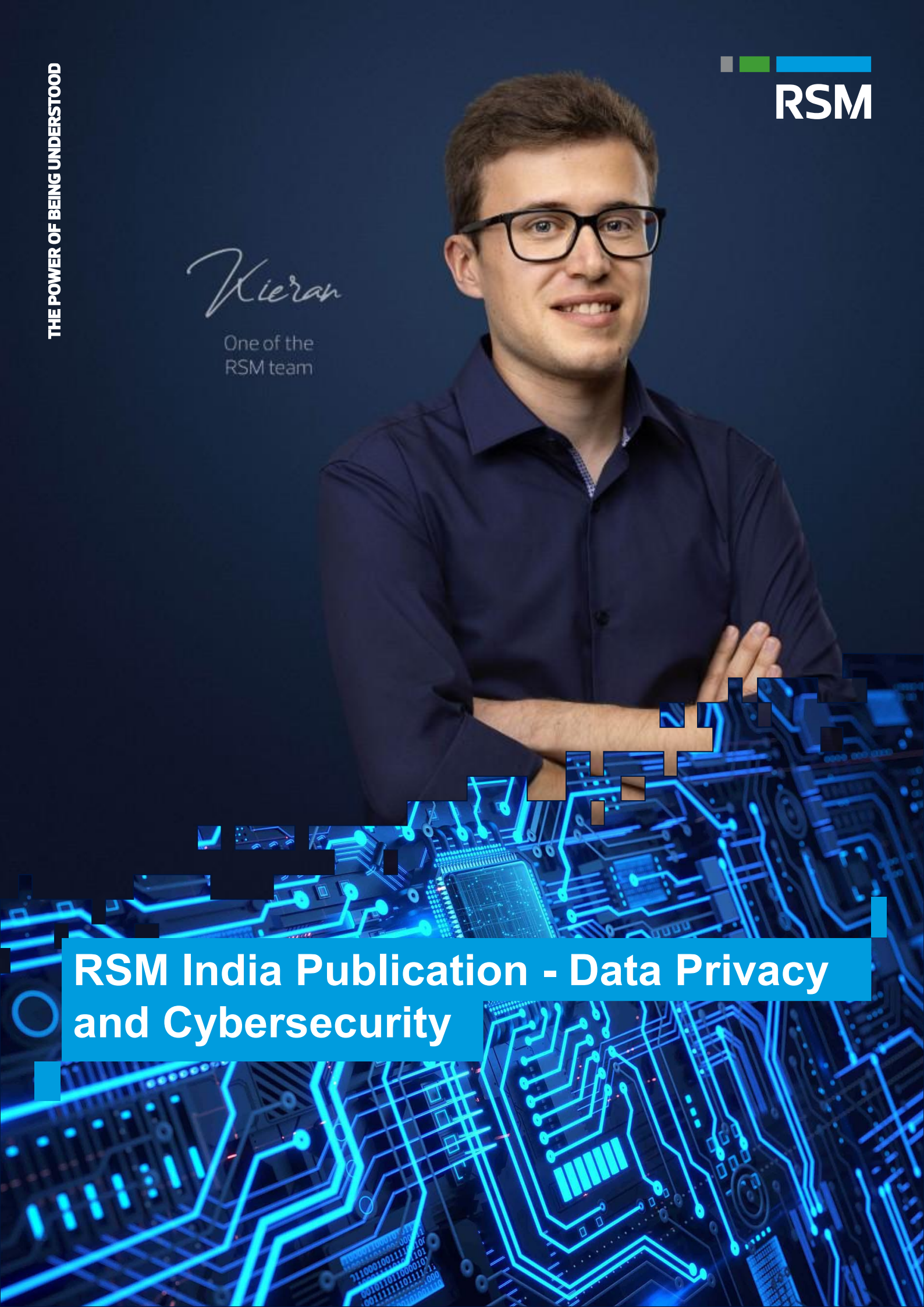
THE POWER OF BEING UNDERSTOOD

RSM



RSM India Publication - Data Privacy and Cybersecurity

RSM IN INDIA

- RSM India (comprising of RSM Astute Consulting Group and affiliates) is consistently ranked amongst India's top tax, accounting and consulting groups [International Accounting Bulletin - India Surveys]
- Nationwide presence through offices in 14 key cities across India
- Multi-disciplinary personnel strength of over 3,000
- International delivery capabilities

rsmindia.in

RSM AROUND THE GLOBE

- Amongst world's leading provider of audit, tax and consulting services to entrepreneurial growth-focused organisations globally
- Annual combined fee income of US$ 10 billion
- Combined staff of over 65,000 in over 900 offices across more than 120 countries

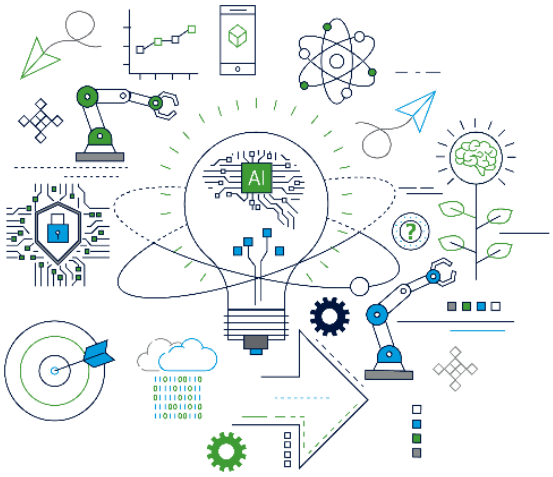
rsm.global

Table of Contents

SECTION A - DATA PRIVACY

Chapter 1: Introduction to Data Privacy

1.1 Definition and Importance



Data privacy, also referred to as information privacy or data protection, involves the proper handling, processing, storage, and dissemination of personal data. It encompasses the relationship between data collection practices, technology, public expectations, contextual information norms, and the legal and political frameworks that govern these activities. The significance of data privacy has increased significantly in recent years due to the exponential increase in the volume and variety of personal information being collected and processed in the digital age.

The importance of data privacy can be understood through several key aspects:

- **Protecting personal information:** Ensures confidentiality and security of sensitive personal data, such as financial records, health information, and personal communications.
- **Maintaining trust:** Builds and sustains trust between individuals and organizations by guaranteeing responsible data handling.
- **Preventing abuse:** Protects against the misuse of personal information, such as identity theft, fraud, and unauthorized surveillance.
- **Compliance:** Ensures adherence to legal and regulatory mandates that require the protection of personal data.

1.2 Historical Context

The concept of data privacy has evolved significantly over time, influenced by technological advancements and the growing digitization of personal information. Various regions worldwide have developed their own frameworks and regulations to address data privacy concerns.

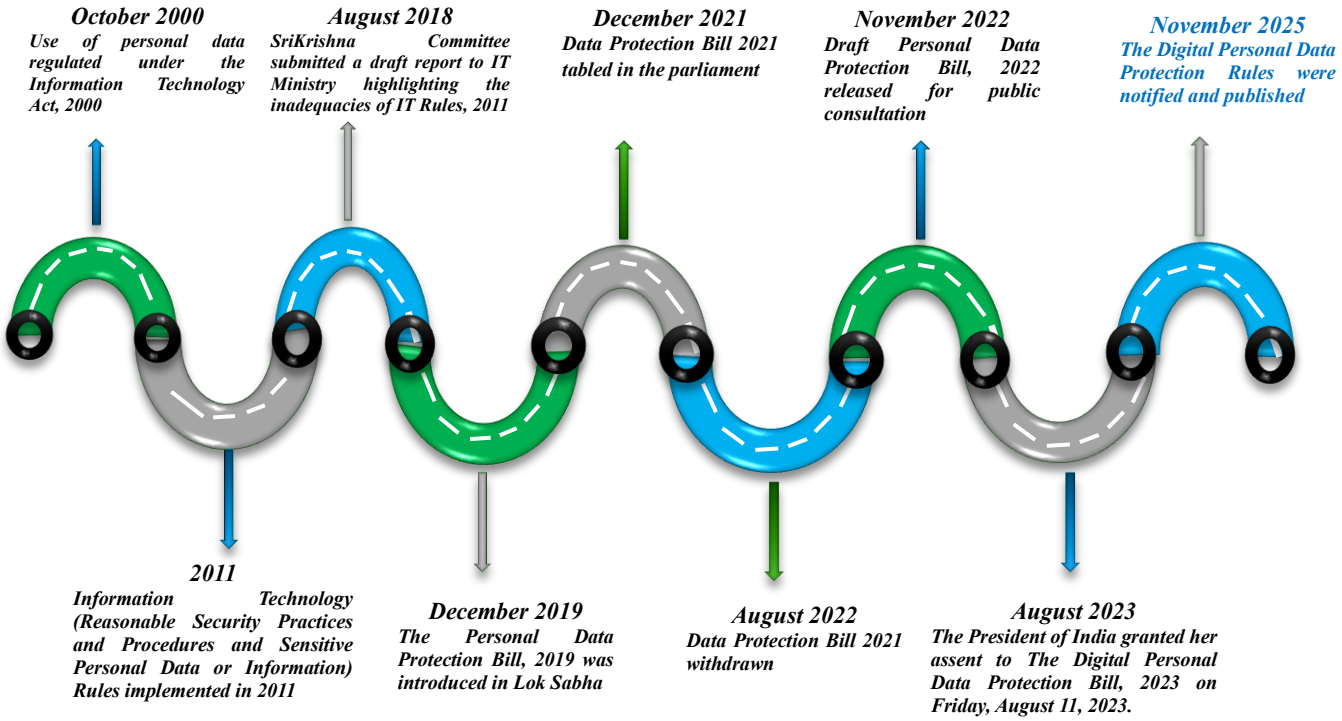
1.3 Global Developments

- **General Data Protection Regulation (GDPR) - European Union:** Enacted in 2018, the GDPR is one of the most comprehensive data protection regulations globally. It sets stringent requirements for data handling and grants extensive rights to individuals regarding their personal data.
- **California Consumer Privacy Act (CCPA) - California:** Effective from 2020, this act provides California residents with substantial control over their personal information, including the right to know what data is collected, the right to delete it, and the right to opt-out of its sale.

India's Digital Personal Data Protection Act:

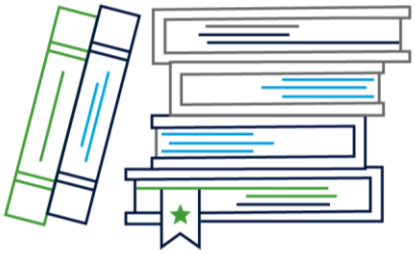
India with over 80 crore internet users, is amongst the highest consumers and producers of data per capita amongst the countries. Digital India has transformed the lives of crores of Indians. With this, personal data security and privacy issues have become very important aspects of our daily interactions and have thus figured prominently across various forums in recent years. On 24th August 2017, a nine Judge Bench of the Supreme Court delivered a unanimous verdict in ***Justice K.S. Puttswamy vs. Union of India*** and other connected matters, affirming that the Constitution of India guarantees to each individual a fundamental right to privacy.

Against this backdrop, it became important to have a law to address the privacy of data. A brief timeline of the Data Privacy regulation in India is as follows:



Chapter2: Digital Personal Data Protection Act (DPDPA)

2.1 Background and Purpose



India's Digital Personal Data Protection Act (DPDPA) was introduced in 2023 to regulate the processing of digital personal data while respecting individuals' right to privacy and processing such data for lawful purposes.

It aims to ensure transparency and accountability in data handling practices, aligning with global data protection standards.

In order to provide the detailed procedures, standards, and operational requirements needed to actually implement and enforce the DPDPA Act, rules were notified and published on November 13, 2025.

2.2 Scope and Applicability

- The Act applies to the processing of digital personal data within the territory of India, where the personal data is collected in:
  - digital form; and
  - non-digital form which is digitised subsequently.
- Also applies to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.
- Shall not apply to:
  - Personal data processed by an individual for any personal or domestic purpose; and
  - Personal data that is made or caused to be made publicly available by:
    a) The Data Principal to whom such personal data relates; or
    b) Any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

    For instance: X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

c) Processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.

- **The rules will be come into force in a phased manner as follows:**

Rules	Effective Date	
Rules 1, 2 and 17 to 21	on the date of their publication in the Official Gazette	November 13, 2025
Rule 4	one year after the date of publication of this Gazette.	November 13, 2026
Rules 3,5-16, 22-23	18 months after the date of publication of this Gazette	May 13, 2027

Basically, Data Principals have 18 months to ensure that the compliances are put in place. Meanwhile, the government is setting-up the Data Protection Board, which will have the authority to levy a penalty through immediate actions under Rules 1,2 and 17 to 21. Though Rule 4 Consent Managers will come into force in 12-month time frame.

2.3 Key Provisions of the DPDPA

2.3.1 Definitions and Core Concepts

The DPDPA introduces several key definitions and concepts essential to understanding its provisions:

"**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.

"**Data Principal**" means the individual to whom the personal data relates and where such individual is—

a. a child, includes the parents or lawful guardian of such a child

b. a person with disability, includes her lawful guardian, acting on her behalf.

"**Data Fiduciary**" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

"**Data Processor**" means any person who processes personal data on behalf of a Data Fiduciary.

"**Digital Personal Data**" means personal data in digital form.

"**Personal Data**" means any data about an individual who is identifiable by or in relation to such data.

"**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.

2.3.2 Grounds for processing personal data: -

a) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,

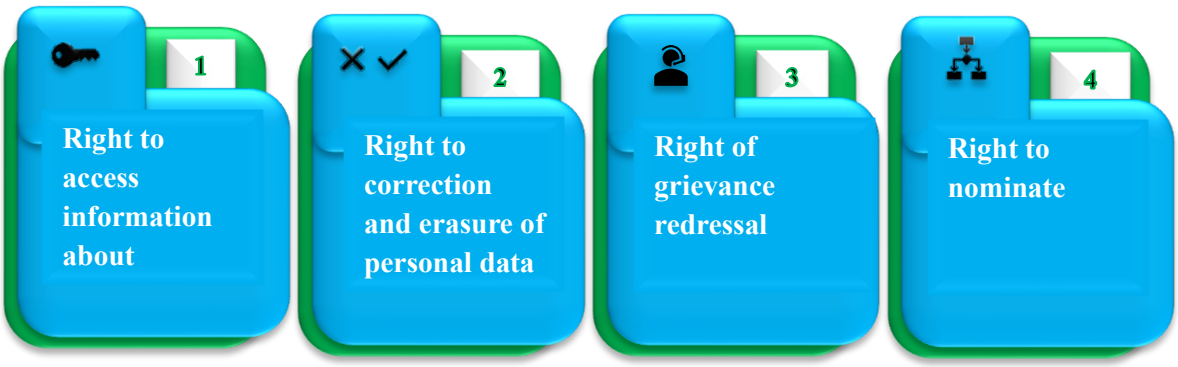
- for which the Data Principal has given his/her consent; or
- for certain legitimate uses.

b) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

2.3.3 Rights of Data Principal

The DPDPA grants several rights to Data Principals, including:

- **Right to access information about personal data:**



Data Principal shall have the right to obtain:

- summary of personal data and processing activities undertaken.
- identifies all other Data Fiduciaries with whom such data is shared, along with a description of the data shared.
- any other info, as may be prescribed by the Act.

- **Right to correction and erasure of personal data:** Data Principal shall have the right to correction, completion, updating and erasure of personal data.

- Data Fiduciary on receiving the request from Data Principal shall correct, update and complete the incomplete data.

- Data Fiduciary shall erase the data on request unless retention is necessary for compliance with any law.

- **Right of grievance redressal:**

  - Data Principal shall have the right to have readily available means of grievance redressal in relation to the personal data.

  - The Data Fiduciary or Consent Manager shall respond to any grievances referred to within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

  - The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.

- **Right to nominate:**

  Data Principal shall have the right to nominate any other individual, in case of death or incapacity (unsound mind or infirmity of body).

Data Fiduciaries (and Consent Managers, where applicable) must **clearly publish** on their website or app:

- **How a Data Principal can request to exercise her rights** under the DPDPA.

- **What identifiers (e.g., username, email, mobile number)** must she provide to be correctly identified.

Data Fiduciaries and Consent Managers must also publish details of their **grievance redressal system** and must be capable of **responding to grievances within 90 days**, supported by appropriate technical and organisational measures.

A Data Principal may nominate another individual to exercise her rights on her behalf, following the Data Fiduciary's terms of service and applicable law, and providing any required identifiers.

2.3.4 Obligations of Data Fiduciaries, Data Principal and Processors

Data Fiduciary	Data Processor	Data Principal	Significant Data Fiduciary
A. Data collection & processing: 1. Provide notice and obtain consent for use of personal data. (Refer consent management process) 2. Use the personal data collected for defined purposes only. 3. Ensure accuracy of personal data. **B. Technical measures:** 4. Implement technical and organizational measures for complying with the Act. 5. Take reasonable measures to prevent data breach. 6. Ensure data erasure on withdrawal of	1. Provide services only under a valid contract with the Data Fiduciary. 2. Erase any personal data on instructions from Data Fiduciary. 3. Protect the data under its possession.	1. Do not suppress material information while providing personal data. 2. Do not register false complaints. 3. Do not impersonate. 4. Do not furnish unverifiable information. 5. Comply with the provisions of the Act.	1. Appoint: • a Data Protection Officer. • an independent data auditor to carry out data audit. 2. Carry out: • Data Privacy Impact Assessment. • Periodic privacy reviews **Note:** The above are in addition to the obligation of Data Fiduciary.

Data Fiduciary	Data Processor	Data Principal	Significant Data Fiduciary
consent/ completion of service. **C. Governance:** 7. Publish business contact information of Data Protection Officer. 8. Appoint data processor under valid contract. 9. Establish effective grievance redressal mechanism. 10. Respond to Data Principals' requests. Ensure to prominently publish on its website or app, or both, as the case may be, (a) details of the means using which a Data Principal may make a request for the exercise of rights; and (b) particulars of identifiers			

Data Fiduciary	Data Processor	Data Principal	Significant Data Fiduciary
required to verify the Data Principal under the terms of service. 11. Refrain from processing personal data that may cause harm to a child, or track them, and obtain parental consent before processing 12. Comply with the provision of this Act			

A Data Fiduciary's notice to a Data Principal must:

- Be presented clearly and stand on its own, without relying on other information provided elsewhere.
- Provide information in plain, easy-to-understand language, enabling the Data Principal to give *specific and informed* consent. This must include at a minimum:
  - A detailed, itemised list of the personal data being collected.
  - The specific purposes for which the data will be processed, including a clear description of the goods/services or uses enabled by the processing.

- Provide a direct communication link to the Data Fiduciary's website or app, and describe any other methods available for the Data Principal to:

- Withdraw consent easily (with the same ease as giving consent).
- Exercise her rights under the Act.
- File a complaint with the Data Protection Board.

Examples for Notice to Data Principal:

- X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening a bank account, X opts for the processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

- X, an individual, have her consent to the processing of her personal data for an online shopping app or website operated by Y, an e-commerce service provider, before the commencement of this Act. Upon commencement of the Act, Y shall, as soon as practicable, give through email, in-app notification or other effective method information to X, describing the personal data and the purpose of its processing.

2.4 Compliance Requirements for Data Fiduciary

2.4.1 Data Collection and Processing

Organizations must adopt practices that ensure data is collected and processed lawfully. This involves:

- Clearly defining the purpose of data collection.
- Ensuring that data collection is limited to what is necessary.
- Processing data in a manner that is consistent with the stated purposes.

2.4.2 Consent Management

Obtaining and managing consent is a critical aspect of compliance:

- Consent must be obtained for all cases except legitimate uses - (Refer Section 4(b) of the Act).
- Organizations must maintain records of consent to demonstrate compliance.
- Organizations shall develop a consent management system to comply with all the requirements stated in the obligations of Data Fiduciary.

Data Fiduciaries can process the personal data of the Data Principal only when:

- Data Principal has given consent or
- Data processing is covered under "Certain legitimate uses"- (Refer Section 4(b) of the Act).

2.4.2.1 Consent Management

- **Consent Mechanism***:* -
  - For obtaining the consent from the Data Principal, Data Fiduciary shall give a notice containing the following information: -
    - The personal data and the purpose for which the same is proposed to be processed.
    - The manner in which consent can be withdrawn.
    - Details of the grievance redressal mechanism.
    - The manner in which Data Principal may make a complaint to the data protection board.

    If the consent is taken before the commencement of the DPDPA, **then a fresh notice needs to be issued in the above manner.**

- **Requisites of consent: -**
  - Consent shall be specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of personal data for the specified purpose and not any other purposes.

    For instance: X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (*i*) the processing of her personal data for making available telemedicine services, and (*ii*) accessing her mobile phone contact list, and X signifies her consent to both. Since a phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services.

    Any part of the consent which constitutes an infringement of the provisions of this Act, or the rules made thereunder, or any other law for the time being in force shall be invalid to the extent of such infringement.

For instance: X, an individual, buys an insurance policy using the mobile app or website of Y, an insurer. She gives her consent to Y for (*i*) the processing of her personal data by Y for the purpose of issuing the policy, and (*ii*) waiving her right to file a complaint to the Data Protection Board of India. Part (*ii*) of the consent, relating to waiver of her right to file a complaint, shall be invalid.

- Shall be presented in clear and plain language, giving the option to access such a request in English or any language specified in the Eighth Schedule to the Constitution.

- Provide the contact details of a Data Protection Officer, where applicable, or of any other person authorized by the Data Fiduciary to respond to any communication from the Data Principal.

■ **Change/withdrawal of consent: -**

- Right to manage, review or withdraw the consent with the same ease as providing the consent.

- If the Data Principal withdraws consent, Data Fiduciary shall cease processing of the data within a reasonable time.

- The consequences of the withdrawal shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

  For instance: X, an individual, is the user of an online shopping app or website operated by Y, an e-commerce service provider. X consents to the processing of her personal data by Y for the purpose of fulfilling her supply order and places an order for the supply of a good while making payment for the same. If X withdraws her consent, Y may stop enabling X to use the app or website for placing orders, but may not stop the processing for the supply of the goods already ordered and paid for by X.

■ **Consent Manager: -**

- The Data Principal may give, manage, review or withdraw consent to the Data Fiduciary through a Consent Manager.

- The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

- Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as are prescribed.

- **Burden of proof: -**

  When a question arises, it is the responsibility of the Data Fiduciary to prove that a notice was given and consent was taken.

2.4.2.2 Certain Legitimate uses: -

Data Fiduciary can process the personal data of Data Principal without consent if the processing falls under any of the following uses: -

- Voluntarily provided by the Data Principal for any specified purpose.

  For instance: X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y with her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt.

- Government services like subsidy, benefits, certificate, license etc.,

  For instance: X, a pregnant woman, enrols herself on an app or website to avail government's maternity benefits programme, while consenting to provide her personal data for the purpose of availing of such benefits. The government may process the personal data of X to determine her eligibility to receive any other prescribed benefit from the government.

- If required by the government under any law.
- For fulfilling any obligation under any law.
- For the compliance of Judgement or Decree or order under any law.
- In case of medical emergencies like COVID or any other pandemic.
- Health services during an epidemic or any other threats to public health.
- For safety during a disaster or any breakdown.
- For purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, intellectual property, classified information, etc.

Regardless of the lawful basis for collecting data (whether it is for legitimate use, consent, legal obligations, etc.), **organizations are required to implement adequate security measures to protect that data from unauthorized access, breaches, and other risks.**

2.4.2.3 Data Security Measures

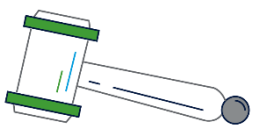
A Data Fiduciary must protect all personal data under its control—whether processed by itself or by a Data Processor—by implementing **reasonable security safeguards** to prevent personal data breaches. At minimum, this includes:

- **Data security measures** such as encryption, masking, obfuscation, or tokenisation.
- **Access controls** over systems and computer resources used by the Data Fiduciary or Data Processor.
- **Monitoring and visibility** through logs, reviews, and audits to detect, investigate, and remediate unauthorized access.
- **Business continuity measures**, such as data backups, to ensure continued processing if data integrity, confidentiality, or availability is compromised.
- **Retention of logs and relevant data for at least one year** to enable detection, investigation, and remediation of security incidents, unless another law requires a different period.
- **Contractual obligations** requiring Data Processors to implement the required security safeguards.
- **Technical and organisational measures** to ensure effective enforcement of all security safeguards. Apart from the above some such measures may include:
    - Conducting regular security audits and vulnerability assessments
    - Obtaining ISO 27001 certification for Information Security Management Systems and ISO 27701 for privacy information management

2.5 Enforcement and Penalties

2.5.1 Regulatory Bodies

The central government has established the Data Protection Board of India for overseeing compliance and enforcing the provisions of the Act. The Board will have the authority to:



- direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire

into such personal data breach and impose a penalty as provided in this Act.

- inquire into such breach and impose a penalty as provided in this Act:
  - on a complaint made by the Data Principal in respect of a personal data breach by a Data Fiduciary or Consent Manager
  - on receipt of information of a breach of any condition of registration of a Consent Manager.
- inquire into such breach and impose a penalty as provided in this Act on a reference made by the Central Government in respect of the breach in observance of the provisions by an intermediary.

2.5.2 Penalties for Non-Compliance

Non-compliance with the DPDPA can result in significant penalties, which are intended to deter violations and promote adherence to data protection standards. Penalties include:

Sr. No	Breach of provisions of this Act or rules made thereunder	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach.	May extend to two hundred and fifty crore rupees.
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach.	May extend to two hundred crore rupees
3	Breach in observance of additional obligations in relation to the processing of personal data of children	May extend to two hundred crore rupees.
4	Breach in observance of additional obligations of a Significant Data Fiduciary	May extend to one hundred and fifty crore rupees.
5	Breach of any other provision of this Act or the rules made thereunder	May extend to fifty crore rupees.

While determining the amount of monetary penalty to be imposed, the Board shall have regard to the following matters, namely:

- the nature, gravity and duration of the breach;
- the type and nature of the personal data affected by the breach;
- repetitive nature of the breach;

- whether the person, as a result of the breach, has realised a gain or avoided any loss;
- whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;
- whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and
- the likely impact of the imposition of the monetary penalty on the person.

2.6 Case Studies and Examples

2.6.1 Practical Implications

Practical implications of DPDPA provisions are as below:

- **E-commerce and online services:** Explicit consent from the users has to be obtained before sending any marketing emails. They must provide clear opt-in options and easy ways for recipients to unsubscribe.
- **Cookie banners:** Websites must inform users about the use of cookies and obtain their consent before storing any non-essential cookies on their devices. Privacy notices in many organizations are silent on the Data Principal's rights and on the collection of children's data.
- **Data Minimization:** Financial institutions must implement data minimization principles, ensuring they only collect data that is necessary for their operations and legal obligations.
- **Data Retention:** Marketing companies must establish clear data retention policies, ensuring personal data is not kept longer than necessary for the purposes for which it was collected.
- **Data Processing Agreements:** Businesses must ensure that third-party service providers processing personal data on their behalf comply with privacy regulations. This includes having data processing agreements in place that outline responsibilities and compliance measures.

2.6.2 Notable Cases and Decisions:

Since the rules and the Act are yet to be fully implemented, currently there are no cases and decisions on non-compliance with this Act. However, below are a few instances of cases under global privacy acts:

- In January 2023, Meta was fined €390 million by the Irish Data Protection Commission for overuse of data for targeted ads by forced consent in violation of GDPR regulations. The company was accused of bypassing GDPR's requirement for explicit consent when it forced its users to accept targeted advertising by making consent a condition for using the platform.

- In September 2023 Irish Data Protection Commission imposed a fine of €345 million on TikTok for violations of platform settings for child users, including family pairing settings, age verification & transparency information for children.

- **The investigation highlighted:**

    - The default setting of TikTok made children's accounts public by default and allowed anyone to view their content, thereby violating GDPR's principles of data minimization and protection by design and default.

    - Family Pairing option allowed non-child users (who could not be verified) to enable direct messaging to children's accounts without their consent. The integrity of children's data becomes questionable in such circumstances.

    - The age verification process of TikTok was deemed inadequate, failing to properly assess the risk of children under 13 accessing the platform.

    - Sufficient information was not provided by TikTok to children about the public-by-default nature of their accounts and the potential audience for their content, failing to meet transparency requirements under GDPR.

- In June 2023, Criteo was fined €40 million for violations related to GDPR, specifically for failure to demonstrate the consent given, right of access, withdrawal of consent and erasure of data of people and agreement with joint controllers for "targeted advertisement." The following points were noted:

    - Citreo relied on its partners to gather consent,but did not implement checks or audits to ensure consent was properly obtained.

    - It did not provide its users full transparency on how their data would be processed.

- It did not erase the users' personal data when the consent was withdrawn.
- Lack of agreement with the joint controller agreement with its partners.

2.7 Comparing DPDPA and GDPR

2.7.1 Key differences

While both the DPDPA and GDPR emphasize the protection of personal data, there are notable differences:

DPDPA	Category	GDPR
DPDPA applies to the processing of digital personal data within the territory of India where the personal data is collected: i. in digital form; or ii. in non-digital form and digitised subsequently;	**Scope**	GDPR applies to the processing of personal data in EU, wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
DPDPA also allows for the processing of personal data for certain 'legitimate uses' for which specific consent is not required: i. Data provided voluntarily by data subjects. ii. Data required for compliance with law. iii. Employment related purposes.	**Legitimate use**	Under GDPR, legitimate interest is one of the 6 lawful bases for processing personal data namely consent, contract, legal obligation, vital interest, public tasks or legitimate interest.
Every request for consent shall be presented to the Data Principal giving the option to access such request in English or any language specified in the Eighth Schedule to the Constitution (22 languages)	**Notice language**	There is no requirement to provide notice in regional languages in GDPR.
Consent Managers are entities registered with the Data Protection Board under the DPDPA and act on behalf of Data Principals to review, provide, manage, and withdraw consent.	**Consent Managers**	There is no equivalent concept under the GDPR.
For processing the personal data of children under the age of 18,	**Personal data of children**	Minors under age 16 need parental consent. Members states

DPDPA	Category	GDPR
consent needs to be taken from parents/ guardian.		of Europe can lower this age to 13 for their regions.
Only Significant Data Fiduciaries are required to conduct periodic Data Privacy Impact Assessment (DPIA)	**DPIA**	Data Controllers need to conduct Data Privacy Impact Assessment (DPIA) for all the high-risk processing activities.
The Act comprises of an additional right to nominate while omitting the right to portability. Timeline to respond to the Data Principal requests has not been specified.	**Nomination**	GDPR does not include right to nominate however provides for the right to portability and organizations have to respond within 30 days to a Data Subject request.
The Act has not yet identified any transfer mechanisms for transferring Personal Data to other countries.	**Cross border data transfers**	GDPR has laid down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules
A Data Fiduciary or class of Data Fiduciaries are designated by the Indian government based on: (a) volume and sensitivity of personal data processed; (b) risk to the rights of the Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order.	**Significant Data Fiduciary**	There is no equivalent concept under the GDPR. However, entities which perform high risk processing activities, may be required to: • Conduct data privacy impact assessments. • Appoint a DPO. • Implement stricter security measures.
Only the Significant Data Fiduciary shall have to appoint DPO as a point of contact for the Data Protection Board	**DPO**	Under the GDPR, a DPO must be appointed if the organization is: • a public authority (except for courts acting in their judicial capacity). • carry out large-scale systematic monitoring of individuals (for example, online behaviour tracking); or • carry out large-scale processing of special categories of data or data relating to criminal convictions and offences.

DPDPA	Category	GDPR
Penalties under the DPDP Act extend up to INR 250 crores.	**Penalties**	Penalties under GDPR extend to 20 million euros, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
The Act and the rules does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA).	**Records**	Data Controller and Data Processor are required to maintain the records of processing activities (ROPA).

2.7.2 Comparative Compliance Strategies

Organizations operating in multiple jurisdictions must develop comprehensive compliance strategies that address the requirements of both the DPDPA and the GDPR. This involves:

- understanding the nuances of each regulation.
- implementing a unified data protection framework that meets the highest standards of both regulations.
- conducting regular audits to ensure ongoing compliance.

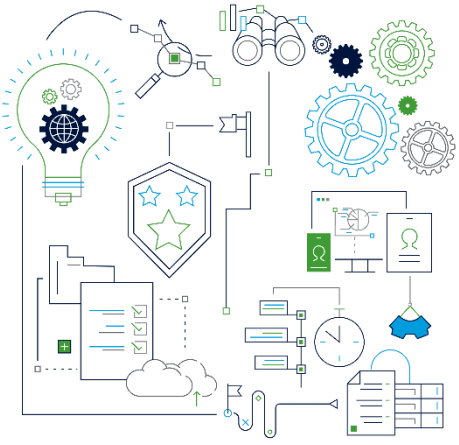
2.8 Impact on Businesses

2.8.1 Operational Implications

Compliance with DPDPA provisions has significant operational impact on day-to-day functions and long-term strategies of the businesses. Key operational impact is enumerated below.

Businesses need to:

- establish policies pertaining to the collection, processing, storage and disposal of personal data.
- create and maintain an inventory of all personal data handled, including data flows and processing activities.
- establish a cross-functional team involving IT, Finance, Legal, HR and operations to ensure a co-ordinated approach to data protection.



- establish processes to ensure that data is used only for purposes specified at the time of obtaining consent.
- invest in new technologies and security measures to facilitate compliance with DPDPA requirements.
- establish a clear process to obtain consent from the Data Principals while ensuring similar ease of process for changing/withdrawing consent.
- train employees on data protection practices and the importance of compliance.
- revise contracts with third-party vendors to include data protection clauses and ensure their compliance with DPDPA.
- appoint a DPO responsible for overseeing compliance with DPDPA, managing data protection activities, conducting Data Privacy Impact Assessments and serving as a point of contact for data subjects and regulators.
- develop and maintain incident response plans to manage and mitigate data breaches.
- establish breach notification procedures to ensure timely notification of breaches to the data protection authorities and affected individuals.

2.8.2 Cross-border data transfers

The DPDPA may impose restrictions on cross-border data transfers to ensure that personal data is adequately protected when transferred outside the country. The Act specifies that the Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India.

2.9 Challenges and Opportunities

2.9.1 Common Challenges in Implementation

Organizations may face several challenges in implementing the DPDPA, which may span across legal, technical, organizational and operational dimensions. Some of the key challenges are as below:

- **Cost of compliance:** The financial burden of implementing data protection measures and technologies.
- **Complexity:** Navigating the complexity of data protection requirements and maintaining ongoing compliance.

- **Ambiguity:** Certain aspects of the Act are open to interpretation, leading to uncertainty about how to comply.

- **Resource allocation:** Allocating sufficient resources and personnel to manage data protection initiatives.

- **Penal exposure:** Organizations may be subjected to huge penalties for non-compliance with this regulation

- **Reputation risk:** Loss of reputation of the business due to non-compliance, resulting in loss of business.

- **Consent management:** Consent management can be particularly challenging in various types of businesses, especially those that handle large volumes of personal data or rely heavily on data processing for their operations. Some examples include:

    - Social Media platforms
    - E-commerce websites
    - Healthcare providers
    - Financial services
    - Telecommunication companies
    - Travel & Hospitality services
    - Education Technology companies
    - Online entertainment & streaming services
    - Online advertising

- **Cross-Border Data Transfer Challenges- Navigating the legal requirements for cross-border data transfers is becoming increasingly complex.**

- **Rules not yet established for the following, resulting in uncertainty with regard to compliance**:

    - class of Data Fiduciaries who may be considered as Significant Data Fiduciary;
    - countries to which transfer of personal data by a Data Fiduciary for processing is restricted.

2.9.2 Opportunities for businesses

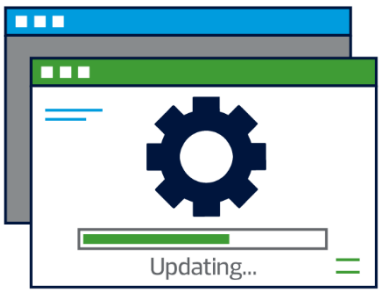
Despite challenges, complying with the DPDPA presents several opportunities:

- **Building trust:** Demonstrating a commitment to data privacy can enhance customer trust and loyalty.
- **Reputation enhancement:** Organizations that prioritize data protection can enhance their reputation and brand image.
- **Competitive edge:** Compliance with data protection regulations can provide a competitive advantage in the marketplace over organizations that are not compliant.

By understanding and implementing the provisions of the DPDPA, organizations can navigate the complexities of data privacy and cybersecurity, ensuring they meet legal requirements while protecting the personal data of individuals in the digital age.

Chapter 3: Future Trends and Development

3.1 Upcoming Regulations and Amendments



As the digital world continues to evolve, so does the regulatory landscape surrounding digital personal data protection. Governments and regulatory bodies are actively working on new regulations and amendments to existing laws, to keep pace with technological advancements and emerging threats.

In many countries, legislative bodies are considering updates to their data protection laws to address the growing complexities of data collection, processing, and sharing. For example, the European Union's General Data Protection Regulation (GDPR) has set a high standard for data protection worldwide, and many nations are crafting their regulations in alignment with or inspired by GDPR principles.

Key areas of focus for future regulations include:

3.1.1 Artificial Intelligence and Machine Learning:

As AI and machine learning technologies become more prevalent, new regulations will likely address the ethical use of personal data in these contexts, ensuring that data-driven algorithms do not compromise individual privacy.

3.1.2 Cross-Border Data Transfers:

With the global nature of data flows, regulations will need to address the complexities of transferring data across borders, ensuring that personal data is protected regardless of where it is processed.

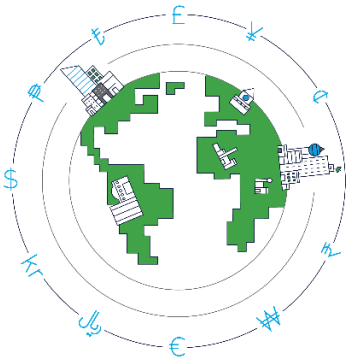
3.1.3 Enhanced Consumer Rights:

Future amendments may introduce new rights for consumers, such as the right to explanation regarding automated decisions and stronger mechanisms for data portability.

3.2 Global Trends in Data Privacy

Data privacy has become a global concern, and countries worldwide are adopting and adapting regulations to protect personal data. Some global trends in data privacy include:

3.2.1 Convergence of Regulations:



More countries are enacting comprehensive data protection laws like the European Union's General Data Protection Regulation (GDPR). Examples include the California Consumer Privacy Act (CCPA) in the U.S., Brazil's General Data Protection Law (LGPD), and India's Digital Personal Data Protection Act (DPDPA). While many regulations share common principles, there are regional variations in terms of scope, enforcement, and specific rights granted to individuals, leading to challenges in global compliance.

3.2.2 Increased Enforcement:

Regulatory bodies are stepping up enforcement actions, imposing significant fines and penalties on organizations that fail to comply with data protection laws. This trend underscores the importance of robust data protection practices.

3.2.3 Public Awareness and Advocacy:

Increased public awareness of data privacy issues has led to greater advocacy for stronger protections. Consumers are becoming more vigilant about their data rights, pushing for more stringent regulations.

3.3 Predictions and Projections

The future of data privacy is poised for significant transformation driven by technological innovation, evolving regulatory frameworks, and changing societal attitudes towards data protection. Some key predictions and projections for the future of data privacy include:

3.3.1 Privacy by Design:

Privacy considerations will become an integral part of the design and development process for new technologies and systems. Organizations will prioritize building privacy features into their products from the outset rather than addressing them as an afterthought.

3.3.2 Decentralized Data Models:

Emerging technologies like blockchain may enable more decentralized data models, giving individuals greater control over their personal data and reducing the risks associated with centralized data storage.

3.3.3 Increased Use of Encryption:

Encryption technologies will become more widespread, ensuring that personal data is protected both in transit and at rest. Advances in quantum computing may also drive the development of new encryption methods.

3.3.4 Emergence of tools to comply with data privacy regulations:

Data privacy tools are essential for ensuring compliance with privacy regulations like the GDPR, DPDP Act, CCPA, and others. Tools for consent management, data storage, data mapping, data masking, impact assessment tools etc., will become more widespread.

3.4 Preparing for Future Challenges

To navigate the future of data privacy effectively, organizations and individuals must prepare for several challenges:

3.4.1 Adapting to Regulatory Changes:

Organizations need to stay informed about evolving regulations and ensure that their data protection practices are compliant. This requires ongoing monitoring and the flexibility to adapt quickly to new legal requirements.

3.4.2 Investing in Privacy Technologies:

Investing in advanced privacy technologies, such as encryption, anonymization, and secure data storage solutions, will be crucial for safeguarding personal data in the face of emerging threats.

3.4.3 Fostering a Privacy-First Culture:

Cultivating a culture that prioritizes data privacy within organizations is essential. This involves educating employees about data protection best practices and ensuring that privacy considerations are embedded in all aspects of operations.

3.4.4 Building Consumer Trust:

Transparency and communication with consumers about data practices will be vital for building and maintaining trust. Organizations should clearly explain how they collect, use, and protect personal data and provide mechanisms for individuals to exercise their data rights.

In conclusion, the future of data privacy is dynamic and multifaceted, shaped by technological advancements, regulatory developments, and societal demands for greater protection. By staying proactive and adaptive, organizations and individuals can navigate this evolving landscape and ensure the continued protection of personal data.

Chapter 4: Practical Implementation Strategies

4.1 Steps to develop a robust framework

Integrating privacy considerations into the design and operation of systems is essential for developing a robust framework. Privacy and Data Protection compliance is a journey and requires ongoing awareness and understanding of personal data processing operations and embedding privacy management throughout the organization. While a one-size-fits-all approach is not feasible, the following key elements based on international leading practices can be considered while formulating a framework.

4.1.1 Data Governance

Establishing data privacy policies, procedures and notices	Establish privacy policy to include, the types of personal data collected, how is the data collected, where will the collected data be stored protected and deleted, data subject rights, grievance redressal mechanism etc. Specific policies for data retention, access controls, breach management etc., should be developed.
Establishing a data breach response plan	Develop and implement a personal data breach management process to address breach incidents and the plan should include appropriate procedures governing all the following key activities, containing the breach, assessing the risk, reporting the incident, evaluating the response, and recovery to prevent future breaches.
Establishing processes for ongoing monitoring	Conduct internal and external audits to ensure compliance with privacy policies and procedures. Implement systems to monitor data access and processing activities.
Cross border data transfer	Review data flow to understand where data is shared cross border. Data can be shared cross border only when there are adequate data protection laws in the country where data is being shared.
Assigning responsibilities	Organizations should look to build Privacy and Data Protection Units responsible for the overall data protection and privacy activities.

4.1.2 Operational & Technical Measures

Mapping the data lifecycle and privacy impact assessments	Understand how personal data flows within the organization—from collection to storage and eventual deletion. This mapping helps identify risks and compliance gaps. Data Privacy Impact Assessment (DPIA) is a process to help identify and minimize the data protection risks of a project or corporate function in the organization.
Reviewing third party relationships	Assess the data protection practices of external partners and vendors. Collaborate with legal advisors or consultants for specialized guidance.
Communicating rights to data subjects	Ensure that individuals are informed about their data rights, including access, rectification, and erasure. Transparency is essential in building trust.
Implementing secure information	Implement technical measures such as encryption, access controls, and intrusion detection systems, anonymization and pseudonymization, data leakage prevention.

4.1.3 Creating awareness & training

Creating awareness on data privacy	Conduct regular training programs on data privacy and security best practices. Employees (full/part time employees, contractors & third parties staff members) should be made aware of their roles and responsibilities towards protecting the organization's information assets and should be aware of key threats to these assets.

4.2 Best Practices & Recommendations

- **Exposure assessment:** The following questionnaire aids in the initial assessment for exposure to DPDPA:

Sr. No.	Initial Assessment Questionnaire
1	Is there an approved a) Data Privacy Policy b) Cyber Security Policy c) Data Retention Policy and Framework d) Incident Management Policy and Breach Notification Process e) Cookie Management Policy?
2	What type of personal data is collected as part of onboarding new customers?
3	During servicing the customer, is the organization exposed to any personally identifiable information (i.e. digital information that can identify a person e.g. mobile number, email address, social security number, PAN card) provided by its customers?
4	Does the organization transfer any personal sensitive data outside India which relates to Indian citizens or vice versa?
5	Does the organization sub-contract any work where sharing personally identifiable information is involved?
6	How is the personal identifiable information collected from employees, vendors and individual shareholders protected?
7	Is there any activity where personal information may be shared to a third party for e.g.: payroll, marketing agency etc.?
8	Is there any vulnerability assessment conducted, and are there any major gaps noted in the report?

- **Process mapping:** Personal data collected as part of business operations needs to be identified, along with the mapping of the journey of such data from collection to destruction. Further, the manner in which data is stored and regular monitoring of access rights to such data needs to be reviewed regularly.

- **Vendor agreements:** Contracts/agreements with vendors to whom personal data is shared for processing, need to contain specific clauses on:

- Clarity on the party responsible for obtaining consent from the data subjects.

- Clarity on indemnification in case of incidence of breach due to vendor's process weaknesses.

- Clarity on the usage of personal data for purposes other than the purpose for which the data is shared.

- **Grievance tracking mechanism:** A robust tool to track all grievances needs to be implemented to ensure adequate defence with the Data Protection Board in the event of any complaint by a third party. The DPO organization can be specifically made responsible for ensuring the same.

- **Analysing children's data:** In businesses such as the travel industry, entertainment industry where it is likely that individuals below the age of 18 visit their websites, it needs to be ensured that data of such individuals are not tracked and used for business intelligence purposes.

- **Data retention:** Data retention period for each category of personal data collected should be defined based on the purpose for which it is collected, and it must be regularly monitored that such data is destructed on completion of such retention period.

- **ISO Certifications:** Consider certifications for ISO 27001- Information Security Management and / or ISO 27701- Privacy Information Management Systems.

- **Internal audits:** Consider coverage of compliance with the DPDP Act through internal audit. Also consider review of data security through Vulnerability Assessment and Penetration (VAPT) Testing.

4.3 The Interplay Between Data Privacy and Cybersecurity

- **How data privacy and cyber security intersect:**

  The interplay between data privacy and cybersecurity is important to understand. While data privacy and cybersecurity have a common goal of protecting sensitive data from unauthorized access, data privacy regulations are prescriptive in nature and important for compliance with local regulations. Cybersecurity prevents personal data from being exposed to external threats. In today's interconnected world, it is not possible to ensure data privacy compliance without ensuring cybersecurity.

- **Ensuring data privacy through cybersecurity:**

  Ensuring data privacy through cybersecurity involves a combination of policies, practices, and technologies designed to protect personal and sensitive information from unauthorized access, disclosure, alteration, and destruction. The following are some key measures to ensure data privacy through security measures:

1. **Developing a cybersecurity strategy:**

   a. Conducting joint risk assessments to identify and evaluate risks related to both cybersecurity and data privacy.

   b. Establishing clear security policies outlining the rules for network access, data protection, incident management, etc.,

   c. Adopting established cybersecurity and data privacy frameworks such as ISO 27001, ISO 27701, NIST etc.,

2. **Implementing robust access controls:**

   a. Enforcing multi-factor authentication for users having access to sensitive systems and data.

   b. Limiting access based on job roles to ensure that users have access only to systems and data required for performing their tasks.

c. Constantly monitoring privilege accounts to prevent misuse.

3. Conducting regular security assessments:

a. Conducting vulnerability assessments to scan and plug vulnerabilities before they are exploited.

b. Performing regular penetration testing to identify and fix vulnerabilities.

c. Ensuring software, applications and operating systems are scanned for updates and patches.

4. Securing the network perimeter:

a. Using firewalls to block unauthorised access.

b. Monitoring network traffic for suspicious activities and preventing intrusions by implementing Intrusion Detection & Prevention Systems

c. Securing remote access to the network through Virtual Private Networks (VPNs) and encrypting communications.

5. Protecting data from unauthorised access:

a. Encrypting data stored on servers, databases, other storage devices and data in transit to prevent unauthorized access.

b. Implementing data loss prevention (DLP) solutions to prevent unauthorized transmission of sensitive data.

c. Maintaining regular backup of critical data and regular testing of disaster recovery plans.

6. Enabling endpoint and device security:

a. Installing and regularly updating antivirus and anti-malware software on all endpoint devices such as computers, mobile devices and servers.

b. Securing and managing mobile devices used by employees to ensure they meet security standards.

7. Implementing a robust incident response plan:

a. Establishing a team of experts for handling breaches and security incidents.

b. Creating a detailed incident response plan detailing the steps to be taken in the event of a cyber incident.

c. Recording learning from the incidents post, addressing the security concerns.

8. Assessing third-party risks:

a. Ensuring third-party service providers adhere to the security standards.

b. Including cybersecurity clauses in contracts with vendors to ensure compliance with data protection regulations and security requirements.

9. Employee training and awareness:

a. Educating employees on cybersecurity best practices, identification of phishing emails, social engineering attacks etc.,

b. Encouraging employees to report suspicious activities and security threat incidents.

c. Sensitize employees on collection, storing and sharing sensitive personal data.

10. Red teaming and blue teaming:

a. Simulating real-world attacks by having red teams perform adversarial testing to identify weaknesses in the systems.

b. Enhancing the organization's ability to detect and respond to attacks by continuously improving monitoring and incident response capabilities.

11. Conducting regular security audits:

a. Conducting regular compliance audits to ensure that applicable regulations on cybersecurity and data privacy are complied with.

b. Enabling necessary tools for logging security incidents on a real-time basis for quick detection and remediation.

12. Continuous monitoring:

a. Enabling necessary tools for logging security incidents on a real-time basis for quick detection and remediation.

b. Leveraging threat intelligence to stay updated on emerging threats, vulnerabilities, and attacker tactics.

4.4 Resources & Appendices

■ Data Privacy Checklist

A comprehensive checklist based on DPDPA is as below for ease of reference:

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
1	**Determine applicability**	N/A	The Act's scope is limited to digital personal data, i.e., personal data collected in digital form or collected offline and later digitized.	1. Does the organization process digital personal data within India? 2. Does the organization process digital personal data outside India, where the processing is related to offering goods or services to Data Principals (data subjects) within India?
2	**Policy & Procedures**	Sec. 4	Data Usage & Protection Policy - Policy containing the rules for collection, usage and protection of data pertaining to Data Principal. Storage, Encryption and Access to the Data	1. Is there a Data Usage and Protection policy defined? 2. Who approved the Data Usage and Protection policy, and what is the timeline of review? 3. Does the policy cover details regarding the data protection principles, data subject's rights, personal data sharing or transfer, consent management, compliance with regulations, complaints & appeals, impact assessment, data breach notifications, etc.
			Data Processing & Retention Policy - Policy containing the rules for	1. Is there a Data Processing & Retention Policy defined? 2. Who approved the Data processing & retention

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			authorization of processing the data for the specified purposes and retention period for the data	policy, and what is the timeline of review? 3. Does the policy cover details regarding the provisions of the DPDP Act, authorization for processing the data, retention period of data used for different types of services?
3	**Employee Training**	N/A	Organization must generate employee awareness for key DPDP requirements and conduct regular training sessions (With periodic evaluations) to ensure that employees remain aware of their responsibilities with regard to the protection of Personal data and detection of personal data breaches. A DPDP awareness program should be a dynamic process that is updated regularly & repeated when a staff-related data breach	1. Whether mandatory training is given to all new joiners (client-facing and others) as part of induction on: • Organization's Data usage & Protection policy. • Organization's Data processing & Retention policy. • Personal data handling and detection of personal data breaches (prior to granting access to the relevant application or information). • Other important compliance requirements? 2. Whether periodic refresher training on the data privacy policy is given to all employees? 3. Is the DPDP training program updated with the latest rules and regulations, and whether the training

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			incident occurs.	manual cover all the relevant information?
4	**Data inventory and data map**		Data Fiduciary shall process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose: a) for which the Data Principal has given her consent; or b) for certain legitimate uses.	1. Has the organization mapped the following: • personal data collected, and how it is collected? • How will it be used? • Where is it stored? • How long will it be stored? • Who is the data owner? • Who will have access to this data? 2. Has the company determined whether the personal data collected is used for legitimate purposes or otherwise?
5	**Consent Management**	Consent Manage-ment	Consent needs to be taken from the Data Principal in accordance with the provisions of the Act, for the purposes for which the data will be used by the Data Fiduciary.	1. Whether consent taken from each Data Principal is maintained by the Data Fiduciary till the time of erasure / withdrawal / completion of service? 2. Does the request made to the Data Principal for consent contain any clause / note that leads to infringement of the provisions of DPDP Act i.e., does it ensure that the consent is free, specific, informed, unconditional,

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				unambiguous, and signifies the agreement to processing personal data for a specific purpose and be limited to such specific purpose? 3. Is the request for consent given in clear and plain language, having the option to access the content in English or 22 other languages specified in the 8th Schedule of the Constitution?
			Every request made for taking the consent from the Data Principal shall be accompanied by a Notice for consent	4. Whether the right to withdraw the consent is provided to the Data Principal? 5. Whether the ease of withdrawing the consent is the same as the ease of providing the consent? 6. What is turnaround time defined between the date of withdrawal of consent and the date of ceasing the data for further use? 7. Whether the organization has approached "Consent Manager" accountable to the Data Principal and such Consent Manager is registered with the Data Protection Board or not?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				8. Whether notice is given for every request made for the consent taken from each Data Principal? 9. If consent is given prior to the application of this Act, whether notice is given to the Data Principal as soon as the Act becomes applicable (within a reasonable time)? 10. Whether notice given along with the consent contains the following particulars? • the personal data that will be collected and the purpose for which the same will be processed. • the manner in which the Data Principal may exercise their right. • the manner in which the Data Principal may make a complaint to the Board.
6	**Legitimate uses**	Sec. 7	Data Fiduciary shall process the personal data of a Data Principal only in accordance with the provisions of this Act and for	1. If the Data Fiduciary is processing the client data without taking the consent from the Data Principal, check whether the purpose of such data processing falls under any of the following:

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			a lawful purpose: a) for which the Data Principal has given her consent; or b) for certain legitimate uses.	• Specified purposes for which data is voluntarily provided by the Data Principal, • Government service, • Is required by the Government or Law or for the compliance of any judgement or decree, or order under any law, • Medical emergency / Health Services during epidemic or any other threats to public health, • Safety during a disaster or any breakdown, • For the purpose of employment (Corporate espionage, Safeguarding IP). 2. Check whether there is segregation between the data being processed with consent and data being processed for legitimate uses, and ensure that data to be processed for legitimate uses does not get processed for the purposes for which consent is required from other Data Principals. 3. Are there controls in place to ensure that data obtained for legitimate uses

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				is also protected against data breaches?
7	**General Obligations of Data Fiduciary**	Sec. 8	A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor	1. Has the Data Fiduciary entered into a valid contract if personal data is shared with Data Processors for processing? 2. Does the agreement contain a clause on responsibility of obtaining consent from the Data Principals, data breach, limitation of liability and usage of personal data only for the purpose specified in the agreement? 3. Does the Data Fiduciary obtain a SOC 2 report from Data Processors to ensure proper IT controls are in place?
8	**Clause 8: - Technological and Organisational measures**	Rule 6	A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act.	Has the organization taken all the technical and organisational measures for the implementation of the provisions of this act: a. Establishing data privacy and cybersecurity policies, b. Security personal data through obfuscation, masking, encrypting data or using the virtual tokens mapped to that personal data,

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				c. Access controls and establishing controls to monitor unauthorized access through logs and controls to prevent recurrence. d. Establish adequate resources to retain logs for a period of one year, e. Establish incident management process, f. Establishing data backup and recovery processes, g. Security endpoint devices, h. Conducting regular employee training, i. Conducting periodic security audits, j. Conducting regular vulnerability assessment and penetration testing.

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
9	**Data Breach**	Sec. 8 Rule 7	A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.	1. Are there any controls designed to identify the data breaches as and when they happen / whether the technology implemented is able to trigger any notification for data breaches? 2. Is there a defined procedure for reporting a potential data breach? 3. Are steps to handle data breaches documented? 4. Is there any data breach register maintained by the organization? 5. Who reviews the data breach register, and what is the frequency of review?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.	6. Does the data breach register contain the status of the breach? 7. Does the Data Fiduciary document any personal data breaches, their effects and the remedial action taken? 8. Is there a mechanism to communicate the data breaches to the Data Principal? 9. Is the TAT defined to communicate data breach to the Data Principal? **For every instance of data breach, verify if:** 10. There is evidence of reporting the same to the Data Principal and the Data Protection Board. 11. The communication was made within the specified time frame of 72 hours. 12. Appropriate measures were taken to mitigate the adverse effects of the breach? 13. Whether the Data Breach notification template/form is maintained to include: 1. description of the breach (nature, extent and timing) 2. consequence of such breach

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				3. measure implemented or being implemented 4. safety measure which a data principal has to take. 5. business contact information of the person who is able to respond on behalf of data fiduciary. 14. How the data breach is notified to the supervisory authority and the data subject?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
10	**Data Erasure**	Sec. 8 Rule 8	A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force: 1. erase personal data, upon withdrawal of consent or the specified purpose is no longer being served, whichever is earlier; and 2. cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for processing to such Data Processor.	1. What is the process to erase personal data once the specified purpose is served? 2. What is the process to erase personal data after the consent is withdrawn by the data subject? 3. Are there any instances of consent withdrawal? 4. Is established process followed to erase such personal data? 5. What controls are put in place to ensure that the outsourced data processor has erased the data on time? 6. Is the organization an e-commerce entity, online gaming intermediary or social media intermediary? If yes: • Is there an adequate mechanism to erase the personal data collected after the purpose is served? • Has the Data Fiduciary given atleast 48 hours' notice before the completion of the time period for erasure to the Data Principal? • the personal data maintained by Data Fiduciary for atleast

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				one year from the date of processing?
11	**Data Protection Officer**	Sec. 8 Rule 9	A Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of their personal data.	1. Whether the Data Fiduciary has appointed a Data Protection Officer, if applicable? 2. Whether the contact information of the Data Protection Officer / person who is able to answer on behalf of the Data Fiduciary is published on the website or app, or both? 3. Whether the Data Protection Officer / such other person appointed has sufficient technical knowledge to address the questions of the Data Principal? 4. Whether the Data Protection Officer / such other person is addressing the queries of Data Principals within a reasonable time?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
12	**Processing of Personal Data of Children and persons with disabilities**	Sec. 9 Rule 10 & 11	Data Fiduciary shall undertake specific measures while processing the personal data of children / person with disability as per the provisions of the Act.	1. Is any personal data of a child / a person with disability processed as part of business activities? 2. Whether verifiable consent from parent / guardian of the child / person with disability is taken for processing of data for the specified purposes in a manner to be prescribed. 3. Ensure that Data Fiduciary has not undertaken any of the following: • processing of data that is likely to cause a detrimental effect on the well-being of the child. • tracking or behavioural monitoring of children or targeted advertising directed at children. 4. Does the organization fall under any of the following categories? • Clinical establishment, • Mental Health establishment • Allied Healthcare Professional • Educational Institution • Creche / Child Day Care Centre Transport services for educational

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				institution, creche or child day care centre. If the response to the above is 'yes', then the following checks are not applicable. Else, • Has the Data Fiduciary verified the consent of the parent / legal guardian before processing any personal data of a child / person with disability? • Has the Data Fiduciary verified the details of identity of an individual identifying themselves as the parent / legal guardian through an identity issued by Central / State Government or entrusted by law?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
13	**Additional Obligations of Significant Data Fiduciary**	Sec. 10 Rule 13	Government may notify a Significant Data Fiduciary based on: a) Volume and sensitivity of personal data b) risk to the rights of the Data Principal c) potential impact on data sovereignty and Integrity of India d) risk to electoral democracy e) Security of the state and f) Public order Significant Data Fiduciary has additional obligations as per the provisions of the Act	1. Verify whether Significant Data Fiduciary (SDF) has appointed a Data Protection Officer representing SDF. 2. Is such a Data Protection Officer based in India? 3. Whether the Data Protection Officer of SDF is reporting to Board of Directors or a similar body of Data Fiduciary? 4. Whether the Data Protection Officer is acting as a point of contact for the grievance redressal mechanism? 5. Whether SDF has appointed an independent data auditor for carrying out the data audit of SDF? Or has the organization voluntarily appointed an auditor to ensure that on-going activities are in compliance with "organisational and technical measures" adopted to protect personal data? 6. Whether SDF has undertaken? • Conducted Data Privacy Impact Assessment (DPIA) every 12 months from the date on which it is notified as SDF?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				• Conducted an audit to ensure compliance with provisions of this Act? • Has submitted the report of DPIA and audit to the Board? • perform due diligence to ensure that software deployed for hosting, displaying, uploading, modifying, publishing, transmission, storage or sharing of personal data processed does not pose any risk to the rights of the Data Principal? • Has the SDF undertaken measures to ensure that personal data specified by the Central Government is not transferred outside the territory of India, which is restricted?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
14	**Rights of Data Principal**	Sec. 11,12,13 ,14 Rule 14	Data Principal shall have the right to access information about personal data	Whether Data Principals, upon making a request, are provided with the information of: • summary of personal data and processing activities undertaken. • identities of all other Data Fiduciaries/Processers with whom such data is shared along with a description of the data shared? • any other prescribed information? Does the organization provide a particular communication link for accessing the website or app, or both, using which the Data Principal may • withdraw their consent • exercise rights under the Act • make a complaint to the Board.

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			Data Principal shall have the right to correction and erasure of personal data	1. Whether Data Principal is provided with the right to request for: • correction, • completion, • updation, • erasure of personal data? 2. Whether the Data Fiduciary has: • corrected • completed, • updated, • erased the personal data on the request of Data Principal? 3. Is the turnaround time defined for addressing the request from Data Principal for correction, completion, updation or erasure of personal data?

Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
			Data Principal shall have the right to grievance redressal	1. Whether Data Fiduciary has set up a grievance redressal mechanism where the Data Protection Officer / Consent Manager is addressing the grievances of Data Principal? 2. Whether the grievance redressal system is readily available to the Data Principal or not on the Data Fiduciary's website or app or both? 3. Whether the grievances are addressed within 90 days by the Data Protection Officer / Consent Manager? 4. Is there any fixed turnaround time for addressing the grievances?
			Data Principal shall have the right to nominate	Whether the Data Principal is provided with the right to nominate any other individual in case of death or incapacity (unsound mind or infirmity of body). ***The manner of nomination is yet to be prescribed under the Act.***
15	**Duties of Data Principal**	Sec. 15	Data Principal, while providing the data for processing, shall comply with the provisions of the Act	Are there any controls to verify: • the authenticity of personal data shared by Data Principal to ensure Data Principal is not impersonating another person. For e.g., verification of phone number through OTP etc.,

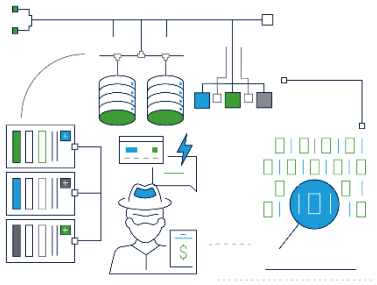
Checklist for Digital Personal Data Protection Act, 2023				
Sr. No.	**Domain**	**Section / Rule**	**Control Objective**	**Control Description**
				• Data Principal has not suppressed any material information while providing their personal data. • Data Principal has not registered any false or frivolous grievance or complaint with a Data Fiduciary or the Board. • Data Principal has routed the grievance through the grievance mechanism channel established by the organization before raising a complaint with the board. • Data Principal furnished accurate data while exercising the right to correction or erasure.
16	**Processing of Personal Data Outside India**	Sec. 16 Rule 15	The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified	1. Whether any data is being transferred to the countries restricted by the Central Government? 2. What controls are put in place to ensure that data transferred to other countries is being used for the specified purposes only and for goods or services rendered in India?
17	**Regulatory changes**		Changes in regulations	Does the company have a mechanism to track changes in the DPDP Act and its rules on an on-going basis?

SECTION B – CYBERSECURITY

Chapter 5: Introduction to Cybersecurity

India's digital transformation has been marked by significant initiatives such as Digital India, Smart Cities Mission, and widespread adoption of digital payment systems. As the country embraces these technological advancements, the importance of robust cybersecurity measures becomes paramount. Cybersecurity threats pose risks to national security, economic stability, and individual privacy.

5.1 Cybersecurity Overview



In an era where digital transformation drives every facet of modern society, cybersecurity emerges as a critical pillar safeguarding our interconnected ecosystem. It transcends mere technical measures, evolving into a multidimensional discipline that encompasses a blend of technology, policy, and human behaviour. The relentless advancement of cyber threats—from sophisticated state-sponsored attacks to pervasive ransomware—necessitates a proactive and adaptive approach to security. Cybersecurity not only defends against breaches and data theft but also fortifies trust in the digital infrastructure that underpins global commerce, communication, and governance. This dynamic field demands continuous innovation and collaboration to anticipate and counteract the evolving tactics of cyber adversaries, ensuring a resilient and secure digital future.

5.1.1 Definition

Cybersecurity is the comprehensive practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage, through the implementation of advanced technologies, rigorous processes, and trained personnel, ensuring the integrity, confidentiality, and availability of information in an increasingly interconnected world.

5.1.2 Need for Cybersecurity

The rapid digitization of India has catalysed unprecedented economic growth and improved access to services. However, it has also expanded the country's vulnerability to cyber threats. This paper examines the current cybersecurity landscape in India, identifies the major challenges, and proposes strategic imperatives to strengthen cybersecurity infrastructure.

Chapter 6: Cybersecurity Landscape and Cyber Threats

The cybersecurity landscape denotes the dynamic and multifaceted environment encompassing the various elements, actors, and factors that influence the security of digital systems and data. It is characterized by a continuous evolution of threats, technological advancements, and regulatory developments. This landscape includes a broad spectrum of components such as threat actors (hackers, cybercriminals, nation-states), types of cyber threats (malware, ransomware, phishing, DDoS attacks), and the defensive measures deployed (firewalls, encryption, intrusion detection systems).

6.1 Cyber Security Landscape

Within the cybersecurity landscape, the interplay between offensive and defensive strategies shapes the overall security posture. Cybersecurity professionals must navigate an ever-changing terrain where new vulnerabilities emerge as technology evolves, requiring constant vigilance, innovation, and adaptation. Moreover, the cybersecurity landscape is influenced by geopolitical dynamics, with cyber warfare and espionage becoming critical elements of national security strategies. Additionally, the landscape is marked by regulatory and compliance requirements that vary across regions and industries, necessitating a deep understanding of legal frameworks and standards. Organizations must not only defend against attacks but also ensure compliance with regulations such as GDPR, HIPAA, and national cybersecurity policies. In essence, the cybersecurity landscape is a complex and ever-shifting domain that demands a holistic approach, integrating technology, policy, and human factors to protect against the myriad of evolving cyber threats.

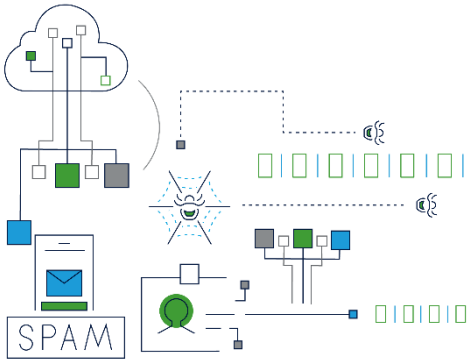
6.2 Major Cyber Threats

Cyber threats are malicious activities or actions aimed at exploiting vulnerabilities in digital systems, networks, and devices to cause harm, disrupt operations, steal data, or gain unauthorized access. These threats are perpetuated by various actors, including cybercriminals, hackers, state-sponsored entities, and insider threats, each with distinct motives ranging from financial gain and political agendas to personal vendettas and corporate espionage.

Cyber threats are diverse and constantly evolving, posing significant risks to individuals, organizations, and nations. Enhancing cybersecurity posture requires a multifaceted approach that includes robust technological solutions, comprehensive policies, continuous monitoring, and ongoing education and training. By understanding and mitigating these major cyber threats, stakeholders can better protect their digital assets and ensure the security and resilience of their operations in the digital age.

6.2.1 Malware and Ransom Attacks

Malware or malicious software encompasses various types of harmful software, including viruses, worms, trojans, ransomware, and spyware. Malware infiltrates systems to steal, encrypt, or delete sensitive data, disrupt operations, or gain unauthorized access to networks.



- **Ransomware:** Encrypts data and demands a ransom for decryption of data.
- **Spyware:** Secretly monitors users and gathers personal information.

Mitigation:

- Use reputable antivirus and anti-malware software.
- Update all systems and software with the latest patches.
- Educate users on recognizing and avoiding phishing emails and suspicious downloads.

6.2.2 Phishing and Social Engineering

Cybercriminals exploit human psychology to deceive individuals into revealing personal information, leading to identity theft and financial losses. Phishing attacks involve cybercriminals sending deceptive emails or messages designed to trick recipients into revealing sensitive information, such as login credentials, financial information, or personal data. These attacks often mimic legitimate communications from trusted sources.

- **Email Phishing:** Fraudulent emails that appear to come from a trusted organization.
- **Spear Phishing:** Phishing attacks targeted at specific individuals or organizations.

Mitigation:

- Implement email filtering solutions to detect phishing emails and take necessary action.
- Conduct regular training sessions for employees on identifying phishing attempts.
- Use multi-factor authentication (MFA) for additional security.

6.2.3 Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks aim to overwhelm a network, server, or website with a flood of traffic, rendering it inaccessible to legitimate users. DDoS disrupts business operations and causes significant financial losses.

- **Volume-Based Attacks:** Overwhelm the target with massive amounts of data.
- **Application Layer Attacks:** Target specific applications or services, exhausting their resources.

Mitigation:

- Use DDoS protection services and solutions.
- Implement robust network architecture with load balancing and redundancy.
- Monitor network traffic for signs of unusual activity.

6.2.4 Advanced Persistent Threats (APTs)

APTs are prolonged and targeted cyber-attacks aimed at stealing sensitive information or compromising critical systems. These attacks are often carried out by well-funded and skilled adversaries, including nation-state actors.

- **Stuxnet:** A highly sophisticated worm that targeted Iran's nuclear facilities.
- **APT10:** A Chinese hacking group known for targeting intellectual property and sensitive data.

Mitigation:

- Employ advanced threat detection and quick response.

- Conduct regular security audits and vulnerability assessments.
- Implement strict access controls and monitor for anomalous activities.

6.2.5 IoT Vulnerabilities

The Internet of Things (IoT) devices have introduced new vulnerabilities that lack robust security features:

- **Mirai Botnet:** Compromised IoT devices to launch large-scale DDoS attacks.
- **Smart Home Hacks:** Exploiting vulnerabilities in smart home devices to gain unauthorized access.

Mitigation:

- Ensure the devices are updated with the latest firmware and security patches.
- Use strong passwords for IoT devices.
- **Segment** / isolate IoT devices from critical systems by providing a separate network.

6.2.6 Cryptojacking

Cryptojacking involves cybercriminals hijacking a target's computational resources to mine cryptocurrencies without their knowledge or consent. This can lead to decreased performance and increased operational costs.

- **Web-Based Cryptojacking:** Malicious scripts embedded in websites that mine cryptocurrency when visited.
- **File-Based Cryptojacking:** Malware that infects devices to perform mining activities.

Mitigation:

- Use anti-malware solutions that detect and block cryptojacking scripts.
- Monitor system performance for signs of unusual activity.
- Educate users on avoiding suspicious websites and downloads.

Chapter 7: Regulatory Bodies and Policy Frameworks

In India, regulatory bodies and policy frameworks play a pivotal role in orchestrating a robust cybersecurity landscape. Entities such as the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC) spearhead initiatives to safeguard the nation's cyber environment. These bodies are instrumental in developing and enforcing comprehensive policies that mandate adherence to security protocols, promote best practices, and facilitate incident response.

Policy frameworks like the National Cyber Security Policy and guidelines under the Information Technology Act provide a structured approach to cybersecurity, addressing the diverse needs of sectors ranging from finance to infrastructure. They establish clear standards for data protection, cyber resilience, and risk management, ensuring a cohesive national strategy. Furthermore, these frameworks encourage collaboration between public and private sectors, fostering an ecosystem of shared knowledge and resources.

By continually updating regulations to keep pace with emerging threats and technological advancements, regulatory bodies and policy frameworks in India ensure a proactive stance against cyber risks, thereby fortifying the country's digital sovereignty and economic stability.

7.1 Regulatory Bodies

India's digital landscape is expanding rapidly, necessitating robust regulatory frameworks to safeguard cyberspace. Various regulatory bodies have been established to oversee cybersecurity, ensure compliance with laws, and respond to cyber threats. India's regulatory bodies play a crucial role in enhancing the country's cybersecurity posture by formulating policies, issuing guidelines, monitoring compliance, and responding to cyber threats. The coordinated efforts of MeitY, CERT-In, NCIIPC, NCCC, RBI, and TRAI ensure a comprehensive approach to cybersecurity, addressing the unique challenges of different sectors and protecting the nation's critical information infrastructure. As cyber threats continue to evolve, these regulatory bodies remain agile and proactive in their efforts to secure India's digital landscape.

7.1.1 Ministry of Electronics and Information Technology (MeitY)

- **Role and Responsibilities:**
  - **Policy formulation:** MeitY is responsible for formulating national policies related to information technology, including cybersecurity policies and strategies.
  - **Implementation and oversight:** It oversees the implementation of cybersecurity measures and initiatives, ensuring adherence to national policies.
  - **Promoting cybersecurity practices**: The ministry promotes best practices, standards, and guidelines for cybersecurity across various sectors.
- **Key Initiatives:**
  - **Digital India Program:** Aims to develop the nation towards a digitally empowered and knowledgeable economy.
  - **Cyber Surakshit Bharat Initiative:** Focuses on raising awareness and building capacities in cybersecurity.

7.1.2 Indian Computer Emergency Response Team (CERT-In)

- **Role and Responsibilities:**
  - **Incident response:** CERT-In acts as the national nodal agency for responding to cybersecurity incidents. It coordinates with various stakeholders to manage and mitigate cyber threats.

- **Threat intelligence and alerts:** It provides threat intelligence; issues alerts and advisories on cyber threats, and disseminates information on vulnerabilities and best practices.
- **Capacity building:** CERT-In conducts training programs, workshops, and exercises to enhance the cybersecurity capabilities of government agencies, private sector entities, and individuals.

■ **Key Initiatives:**

- **Cyber Swachhta Kendra:** A Botnet Cleaning and Malware Analysis Centre aimed at detecting and removing botnet infections.
- **Cybersecurity Drills:** Regularly conducts national and international cybersecurity drills to test and improve incident response capabilities.

7.1.3 National Critical Information Infrastructure Protection Centre (NCIIPC)

■ **Role and Responsibilities:**

- **CII protection:** NCIIPC is tasked with the protection of Critical Information Infrastructure (CII) in India, which includes sectors such as banking, finance, telecommunications, energy, and defence.
- **Risk assessment and management:** Conducts risk assessments, vulnerability analyses, and implements measures to protect CII from cyber threats.
- **Coordination and collaboration:** Collaborates with sectoral CERTs, government agencies, and private sector entities to ensure a coordinated approach to CII protection.

■ **Key Initiatives:**

- **Sectoral CERTs:** Establishment of sector-specific Computer Emergency Response Teams to address unique cybersecurity challenges in different CII sectors.
- **Information Sharing:** Facilitates the sharing of threat intelligence and best practices among stakeholders.

7.1.4 National Cyber Coordination Centre (NCCC)

■ **Role and Responsibilities:**

- **Real-Time monitoring:** NCCC provides real-time situational awareness of cyber threats by monitoring and analysing cyber activities across the country.
- **Coordination and response:** Coordinates responses to cybersecurity incidents, ensuring timely and effective action.
- **Threat analysis and intelligence:** Analyses cyber threats and disseminates intelligence to relevant stakeholders for proactive threat mitigation.

- **Key Initiatives:**

  - **Cyber Threat Analysis:** Conducts continuous monitoring and analysis of cyber threats to provide actionable intelligence.
  - **Incident Coordination:** Facilitates coordination among various agencies and stakeholders during cyber incidents.

7.1.5 Reserve Bank of India (RBI)

- **Role and Responsibilities:**

  - **Regulation of financial sector:** RBI oversees cybersecurity in the banking and financial sector, ensuring that banks and financial institutions implement robust cybersecurity measures.
  - **Guidelines and standards:** Issue guidelines and standards for cybersecurity practices in the financial sector, including requirements for risk assessment, incident response, and data protection.
  - **Supervision and audits:** Conducts regular audits and inspections to ensure compliance with cybersecurity guidelines.

- **Key Initiatives:**

  - **Cybersecurity Framework for Banks:** Establishes a comprehensive cybersecurity framework for the banking sector, focusing on risk management, incident response, and governance.
  - **Cyber Drills and Simulations:** Conducts cyber drills and simulations to test and improve the cybersecurity readiness of financial institutions.

7.1.6 Telecom Regulatory Authority of India (TRAI)

- **Role and Responsibilities:**

  - **Regulation of telecom sector:** TRAI regulates cybersecurity practices within the telecommunications sector, ensuring the security of telecom networks and services.
  - **Standards and guidelines:** Develops and enforces standards and guidelines for securing telecom infrastructure and protecting consumer data.
  - **Monitoring and compliance:** Monitors compliance with cybersecurity regulations and takes corrective actions as necessary.

- **Key Initiatives:**

  - **Telecom Security Guidelines:** Issuance of guidelines for the security of telecom networks and services.
  - **Consumer Awareness:** Promotes awareness among consumers about cybersecurity risks and best practices.

7.2 Policy Frameworks

India has made substantial progress in developing its cybersecurity framework. Key initiatives include the establishment of the Indian Computer Emergency Response Team (CERT-In), the National Cyber Security Policy 2013, and various sector-specific guidelines. Despite these efforts, the country continues to face numerous cybersecurity challenges.

7.2.1 National Cybersecurity Policy, 2013

The National Cybersecurity Policy of 2013 is a comprehensive framework established by the Government of India aimed at protecting the country's information infrastructure and managing the associated risks. This policy was introduced in response to the increasing threat landscape and the need for a robust cybersecurity strategy to safeguard critical information infrastructure.

- **Objectives of the Policy:**

i. **To create a secure Cyber Ecosystem:** The policy emphasizes the creation of a secure and resilient cyber ecosystem within the country. This involves establishing necessary regulatory frameworks, enabling legal, technical, and operational measures to address cyber threats.

ii. **Enhancing capacities:** A key goal is to enhance the capabilities of various stakeholders, including government entities, businesses, and individuals, to effectively respond to and mitigate cyber threats. This includes training and awareness programs aimed at improving the cybersecurity posture.

iii. **Strengthening regulatory frameworks:** The policy aims to strengthen existing legal frameworks to address the issues of cybercrime more effectively. This includes updating laws, improving enforcement mechanisms, and ensuring international cooperation.

iv. **Promoting research and development:** Encouraging R&D in cybersecurity technologies is a significant component of the policy. This involves supporting innovation and the development of new technologies to counter evolving cyber threats.

v. **Protection of Critical Information Infrastructure (CII):** The policy prioritizes the protection of CIIs such as banking, telecommunications, defence, energy, and other vital sectors. It

aims to develop a robust framework for identifying, assessing, and mitigating risks to these infrastructures.

- **Key Components:**

  i. **Institutional Structures:** The policy calls for the establishment of various bodies and institutions to oversee and implement cybersecurity measures. This includes the National Critical Information Infrastructure Protection Centre (NCIIPC), responsible for securing critical information infrastructure.

  ii. **Cybersecurity Assurance Framework:** It includes the development of frameworks to ensure that all entities handling critical data comply with prescribed cybersecurity standards and best practices.

  iii. **Public-Private Partnerships:** Recognizing the role of private sector entities in managing and operating critical infrastructure, the policy promotes collaboration between public and private sectors for effective cybersecurity management.

  iv. **Information Sharing and Cooperation:** The policy encourages the creation of mechanisms for sharing threat intelligence and information on vulnerabilities among various stakeholders, both nationally and internationally.

  v. **Capacity Building and Skill Development:** It stresses the need for enhancing the skills of professionals working in the field of cybersecurity through specialized training programs and certifications.

- **Challenges and Implementation:**

  While the National Cybersecurity Policy, 2013, sets a robust foundation for securing India's cyberspace, its implementation has faced several challenges. These include:

  i. **Coordination among stakeholders:** Ensuring effective coordination among various government agencies, private sector entities, and international partners remains a complex task.

  ii. **Resource constraints:** Allocating sufficient resources, both financial and human, to implement various measures outlined in the policy has been challenging.

  iii. **Rapid technological advancements:** Keeping up with the fast-paced evolution of cyber threats and technologies requires continuous updates to the policy and associated frameworks.

iv. **Awareness and training:** Ensuring widespread awareness and training across all levels of society, from government officials to the general public, is an ongoing effort.

The National Cybersecurity Policy, 2013, marks a significant step towards building a secure and resilient cyberspace in India. It lays down a comprehensive strategy for addressing the multifaceted challenges of cybersecurity. While the policy provides a strong foundation, continuous efforts in terms of coordination, resource allocation, and adaptation to emerging threats are essential for its successful implementation and for safeguarding India's critical information infrastructure.

7.2.2 Information Technology Act, 2000

The Information Technology Act, 2000, is a landmark legislation in India that provides a legal framework for electronic governance and addresses issues related to cybercrime and electronic commerce. Enacted on October 17, 2000, this act represents a crucial step towards adapting the country's legal framework to the digital age, ensuring that electronic transactions are legally recognized and protected.

- **Objectives of the IT Act:**

  i. **Legal recognition of electronic transactions:** One of the primary objectives of the IT Act, 2000, is to provide legal recognition to electronic records and digital signatures, thereby facilitating electronic commerce and transactions.

  ii. **Prevention of cybercrime:** The Act addresses various types of cybercrimes, including hacking, identity theft, and digital fraud, laying down penalties and punishments for offenders.

  iii. **Promoting E-Governance:** The IT Act promotes the use of electronic records and digital signatures in government operations and services, enhancing efficiency and transparency.

  iv. **Facilitating E-Commerce:** By recognizing electronic contracts and transactions, the Act aims to boost the growth of e-commerce, providing a secure and reliable environment for digital business activities.

- **Key Provisions of the IT Act:**

  i. **Legal recognition of electronic records:** Sections 4 and 5 of the Act grant legal recognition to electronic records and digital signatures, enabling their use in legal contracts, agreements, and other formal documents.

  ii. **Digital signatures:** The Act defines digital signatures and outlines the process for their authentication, making them equivalent to

handwritten signatures in electronic transactions.

iii. **Regulation of Certifying Authorities:** The Act establishes a framework for the regulation of certifying authorities, which are responsible for issuing digital certificates and ensuring the security of digital signatures.

iv. **Cybercrimes and penalties:** Chapter XI of the Act specifies various cybercrimes and prescribes penalties and punishments for offences such as hacking, unauthorized access, identity theft, and cyber terrorism.

v. **Adjudication of disputes:** The Act provides for the appointment of adjudicating officers to handle disputes related to electronic transactions and cybercrimes, ensuring a streamlined process for resolution.

vi. **Establishment of the Cyber Appellate Tribunal:** The Act establishes the Cyber Appellate Tribunal to hear appeals against the orders of adjudicating officers, providing a higher level of judicial oversight.

vii. **Offences by Intermediaries:** The Act outlines the liability of intermediaries, such as internet service providers and web hosting services, for third-party content. It provides them with a safe harbour if they follow due diligence and take necessary actions upon receiving complaints.

- **Amendments and updates:**

  The IT Act, 2000, has undergone several amendments to address the evolving nature of cyber threats and technological advancements. The most significant amendment came in 2008, which introduced several new provisions, including:

  i. **Cyber Terrorism:** The act now includes provisions to address cyber terrorism, defining it and prescribing severe penalties for those involved in cyber terrorism activities.

  ii. **Obscenity and Pornography:** The amendment expanded the scope of the Act to include offences related to the publication and transmission of obscene material, including child pornography.

- **Challenges:**
  Despite its comprehensive nature, the IT Act, 2000, has faced several challenges and criticisms:

  i. **Ambiguity and interpretation:** Some provisions of the Act have been criticized for being vague and open to interpretation, leading to potential misuse and arbitrary enforcement.

ii. **Implementation and enforcement:** Effective implementation and enforcement of the Act's provisions remain a challenge due to a lack of awareness, inadequate resources, and technical expertise among law enforcement agencies.

The Information Technology Act, 2000, serves as a foundational legal framework for governing electronic transactions and combating cybercrime in India. It has played a pivotal role in fostering the growth of e-commerce, promoting e-governance, and enhancing cybersecurity. However, continuous efforts to update and refine the Act are essential to address emerging cyber threats and technological advancements, ensuring that it remains relevant and effective in the digital age.

7.2.3 National Cybersecurity Strategy, 2020

The National Cybersecurity Strategy, 2020, represents a significant step forward in India's efforts to secure its cyberspace against evolving threats. This strategy, developed by the National Security Council Secretariat (NSCS), aims to create a safe, secure, and resilient cyberspace for citizens, businesses, and the government.

- **Objectives of the Strategy:**

i. **Secure National Cyberspace:** The primary goal is to secure India's cyberspace from cyber threats by enhancing the protection of critical information infrastructure and creating a robust cybersecurity framework.

ii. **Strengthen institutions and capacities:** The strategy aims to build and strengthen institutions and capacities across sectors to respond effectively to cybersecurity incidents.

iii. **Promote cyber awareness and skills:** Enhancing cyber awareness among citizens and promoting the development of skills and competencies in cybersecurity is a key focus.

iv. **Foster international cooperation:** The strategy emphasizes the importance of international cooperation in tackling cyber threats and establishing norms for responsible state behaviour in cyberspace.

- **Key Pillars of the Strategy:**

i. **Critical Information Infrastructure (CII) protection:** The strategy outlines measures to identify and protect CII sectors such as banking, telecommunications, energy, and defence. This includes regular risk assessments, vulnerability management, and the establishment of robust incident response mechanisms.

ii. **Institutional framework and governance:** Strengthening the existing institutional framework, including the role of agencies like the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC), to ensure a coordinated response to cyber incidents.

iii. **Capacity building and skill development:** Developing a skilled cybersecurity workforce through education, training, and certification programs. This includes integrating cybersecurity education into school and university curricula and promoting research and development in cybersecurity technologies.

iv. **Cybercrime prevention and law enforcement:** Enhancing the capabilities of law enforcement agencies to prevent, detect, investigate, and prosecute cybercrimes. This involves updating legal frameworks, improving digital forensics capabilities, and fostering cooperation with international law enforcement agencies.

v. **Public-Private partnership:** Encouraging collaboration between government and private sector entities to share information on threats and vulnerabilities and to develop joint strategies for protecting cyberspace.

vi. **Cyber hygiene and awareness:** Promoting cyber hygiene practices among individuals and organizations to prevent cyber incidents. This includes public awareness campaigns, workshops, and the dissemination of best practices for cybersecurity.

vii. **International engagement:** Engaging with international partners to share best practices, participate in global cybersecurity initiatives, and contribute to the development of international norms and standards for cybersecurity.

7.2.4 Strategic Actions and Initiatives

- **National Cybersecurity Coordination Centre (NCCC):** Operationalizing the NCCC to provide real-time situational awareness and coordinate responses to cybersecurity incidents.

- **Cybersecurity training and certification:** Establishing national-level programs for cybersecurity training and certification to ensure a steady pipeline of skilled professionals.

- **Sectoral CERTs:** Creating sector-specific Computer Emergency Response Teams (CERTs) to address unique cybersecurity challenges in different sectors.

- **Research and innovation:** Promoting research and innovation in cybersecurity through funding, grants, and partnerships with academic institutions and industry.

- **Legislative measures:** Reviewing and updating existing cybersecurity laws and regulations to address emerging threats and challenges. This includes developing a robust data protection framework.

- **Challenges and Implementation:**

  The implementation of the National Cybersecurity Strategy, 2020, faces several challenges:

  i. **Coordination and collaboration:** Ensuring effective coordination among various stakeholders, including government agencies, private sector entities, and international partners.

  ii. **Resource allocation:** Allocating adequate resources, both financial and human, to implement the strategy's initiatives effectively.

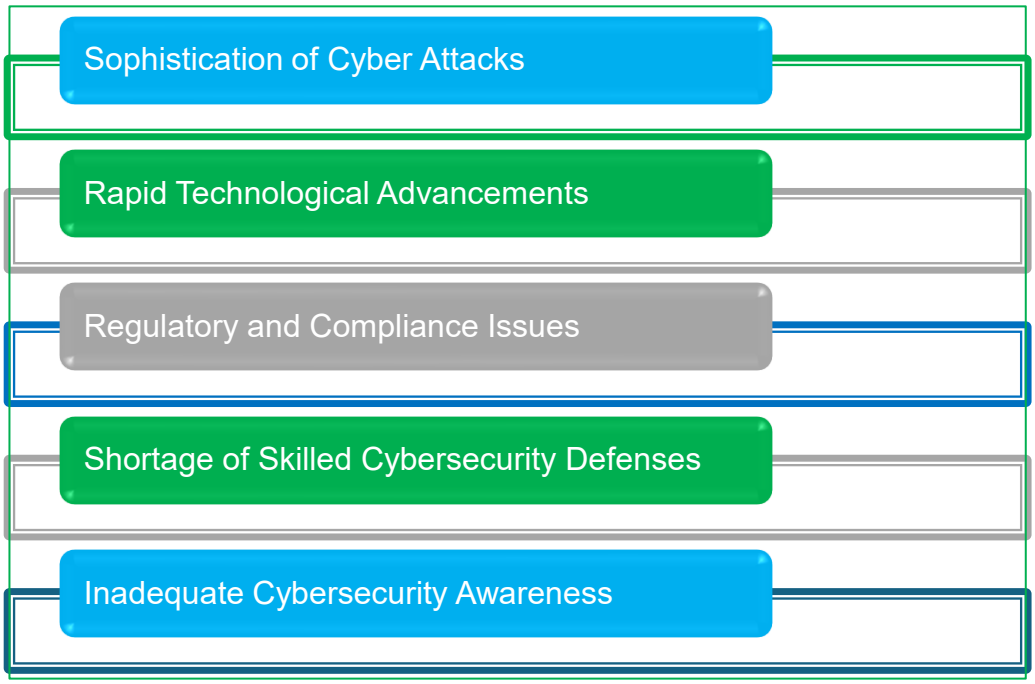
  iii. **Rapid technological changes:** Keeping pace with the fast-evolving cyber threat landscape and technological advancements.

  iv. **Awareness and education:** Promoting widespread awareness and understanding of cybersecurity among the general public and organizations.

  The National Cybersecurity Strategy, 2020, is a comprehensive framework aimed at securing India's digital infrastructure and ensuring a resilient cyberspace. By focusing on critical information infrastructure protection, capacity building, public-private partnerships, and international cooperation, the strategy aims to create a robust cybersecurity ecosystem. Successful implementation of this strategy is essential to protect national interests, promote economic growth, and safeguard the digital lives of Indian citizens in an increasingly interconnected world.

Chapter 8: Challenges in Cybersecurity

While there are multiple cybersecurity policies and guidelines, their implementation and enforcement are inconsistent across sectors. The pace of technological change outstrips the development of corresponding security measures, creating vulnerabilities that can be exploited by cybercriminals. A significant portion of the population remains unaware of basic cybersecurity practices. This lack of awareness extends to small and medium enterprises (SMEs), making them easy targets for cyberattacks.



Chapter 9: Enhancing Cybersecurity Posture

Cybersecurity posture refers to the overall strength and readiness of an organization or a nation to protect its information assets and respond to cyber threats. It encompasses the policies, procedures, technologies, and human resources dedicated to securing digital infrastructure. As India rapidly embraces digital transformation across various sectors, enhancing cybersecurity posture has become a national imperative. The country's growing digital footprint, driven by initiatives like Digital India, e-Governance, and increased internet penetration, necessitates a robust and dynamic approach to cybersecurity.

Key strategies for enhancing cybersecurity posture in India:

- **Strengthening Regulatory Frameworks:**
  - **Data Protection legislation:** Enactment of comprehensive data protection laws to safeguard personal and sensitive data. While the Digital Personal Data Protection Act has been formulated, specifying rules to ensure proper implementation is in progress.
  - **Regular audits and compliance:** Mandatory cybersecurity audits and compliance checks for critical sectors to ensure adherence to established security protocols.
- **Capacity Building and Skill Development:**
  - **Cybersecurity education:** Incorporating cybersecurity education into school and university curricula to build a future-ready workforce. Specialized courses and certifications for professionals to enhance their skills.
  - **Training programs:** Conducting regular training programs for government officials, law enforcement, and private sector employees to stay updated on the latest cybersecurity practices and technologies.
- **Public-Private Partnerships:**
  - **Collaborative frameworks:** Establishing collaborative frameworks for information sharing and joint initiatives between the government and private sector. This includes threat intelligence sharing, joint incident response exercises, and collaborative research projects.

- **Industry engagement:** Encouraging industry associations to develop sector-specific cybersecurity guidelines and best practices.

- **Technological Advancements:**
  - **Advanced security technologies:** Adoption of advanced technologies such as artificial intelligence, machine learning, and blockchain to enhance threat detection, incident response, and data integrity.

  - **Secure infrastructure:** Investment in secure and resilient infrastructure, including secure data centres, encrypted communication channels, and robust network security measures.

- **Critical Information Infrastructure (CII) Protection:**

  - **Risk assessment and management:** Regular risk assessments and vulnerability analyses of critical information infrastructure to identify and mitigate potential threats.

  - **Sectoral CERTs:** Establishment of sector-specific Computer Emergency Response Teams (CERTs) to address unique cybersecurity challenges in critical sectors like finance, healthcare, energy, and defence.

- **Cyber Hygiene and Awareness:**

  - **Public awareness campaigns:** Nationwide campaigns to promote cyber hygiene practices among citizens, businesses, and government employees. This includes awareness on phishing, secure password practices, and recognizing cyber threats.

  - **Best practices dissemination:** Development and dissemination of cybersecurity best practices guides and toolkits for various stakeholders.

- **Incident Response and Recovery:**

  - **Incident response teams:** Formation of dedicated incident response teams at national and organizational levels to handle cybersecurity incidents promptly and effectively.

  - **Recovery plans:** Development of comprehensive incident response and disaster recovery plans to ensure quick recovery from cyber incidents and minimize impact.

- **International Cooperation:**

  - **Global partnerships:** Active participation in global cybersecurity initiatives and collaborations with international organizations and countries to share best practices and tackle cross-border cyber threats.

- **Norms and standards:** Contributing to the development of international norms and standards for responsible state behaviour in cyberspace.

- **Challenges and Opportunities:**

  - **Challenges:**

    a. **Resource constraints:** Limited financial and human resources dedicated to cybersecurity can hinder the implementation of robust security measures.

    b. **Evolving threat landscape:** Rapidly changing cyber threats require continuous adaptation and updating of security strategies and technologies.

    c. **Awareness gap:** A significant gap in cybersecurity awareness among the general public and small businesses, making them vulnerable to cyber-attacks.

  - **Opportunities:**

    a. **Technological innovations:** Leveraging emerging technologies to enhance cybersecurity measures and develop innovative solutions to tackle cyber threats.

    b. **Government initiatives:** Leveraging government initiatives like Digital India and Startup India to promote cybersecurity startups and innovation.

    c. **Global leadership:** Establishing India as a global leader in cybersecurity through active participation in international forums and setting high standards for cybersecurity practices.

Chapter 10: Conclusion – Cybersecurity

Enhancing India's cybersecurity posture is crucial for safeguarding its digital economy, protecting critical infrastructure, and ensuring the security of its citizens in an increasingly digital world. By strengthening regulatory frameworks, building capacity, fostering public-private partnerships, embracing technological advancements, and promoting cyber awareness, one can create a robust and resilient cybersecurity ecosystem. Addressing the challenges and leveraging opportunities will be key to achieving this goal.

■ Responsibility to Manage Cybersecurity

- Managing cybersecurity in an organization is a multifaceted responsibility that involves various roles, departments, and stakeholders working together to protect the organization's digital assets and data. While the ultimate accountability for cybersecurity often lies with top leadership, several key roles and functions are crucial to maintaining a robust cybersecurity posture.

- In today’s interconnected world, cybersecurity is not solely the responsibility of the IT or security departments; it’s a collective effort that involves every individual within an organization. Effective cybersecurity management is a shared responsibility across all levels of an organization. Executives provide the leadership and resources, IT and security teams implement and monitor defences, managers enforce policies, and employees adhere to best practices and report issues. By working together, everyone can contribute to a robust security posture, protecting the organization from the ever-evolving landscape of cyber threats.

RSM India

Mumbai (Corporate Office)
96-97, 9th Floor,
Maker Chambers VI,
Nariman Point,
Mumbai – 400021

3rd floor, Technopolis Knowledge Park, A Wing, MIDC
Andheri East, Mumbai - 400 093

Navi Mumbai
1201A, Rupa Renaissance
Juinagar, MIDC Road
Navi Mumbai - 400 705

New Delhi - NCR
4th Floor, 407, Time Tower,
Mehrauli Gurugram Road,
Sushant Lok Phase 1,
Gurugram – 122 002

1st, 2nd & 3rd floor, B37, Sector 1
Noida - 201 301

Chennai
2nd & 4th floor, Apex Towers
R.A. Puram, Chennai - 600 028

Bengaluru
3rd floor, Jubilee Building
45, Museum Road
Bengaluru - 560 025

Hyderabad
1208, Gowra Fountainhead,
Huda Techno Enclave, Hitec City, Hyderabad - 500 081

Kolkata
5th floor, J K Millennium Centre
Jawaharlal Nehru Road
Kolkata - 700 071

Surat
RSM House, DTA-2
G-02 to G-05 Plot
Gujarat Hira Bourse
Ichhapore-2, Surat - 394 510

Ahmedabad
B/211, 2nd floor, Mondeal Heights
Opp. Karnavati Club, S.G. Highway
Ahmedabad - 380 015

Pune
603, Pride House
Ganesh Khind Road
Opp. NIC University Chowk
Pune - 411 016

Gandhidham
206, Sunshine Arcade II
Plot No. 37, Sector 8
Near D-Mart
Gandhidham - 370 201

Jaipur
101/102, 1st Floor, UDB Tower,
University Marg, Bapu Nagar,
Jaipur - 302 015

Vijayanagar
A2/UT-F, Power Valley
JSW Steel Township Toranagullu
Bellary - 583 123

THE POWER OF BEING UNDERSTOOD

RSM

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

301–307, 3rd Floor, Technopolis Knowledge Park, Mahakali Caves Road, Chakala, Andheri East, Mumbai 400 093

T: (91-22) 6108 5555/ 6121 4444
F: (91-22) 6108 5556/ 2287 5771

E: emails@rsmindia.in **W:** www.rsmindia.in

Offices: Mumbai, New Delhi - NCR, Chennai, Kolkata, Bengaluru, Navi Mumbai, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Jaipur and Vijayanagar.


facebook.com/RSMinIndia


twitter.com/RSM_India


linkedin.com/company/rsm-india


Youtube.com/c/RSMIndia

February 2026