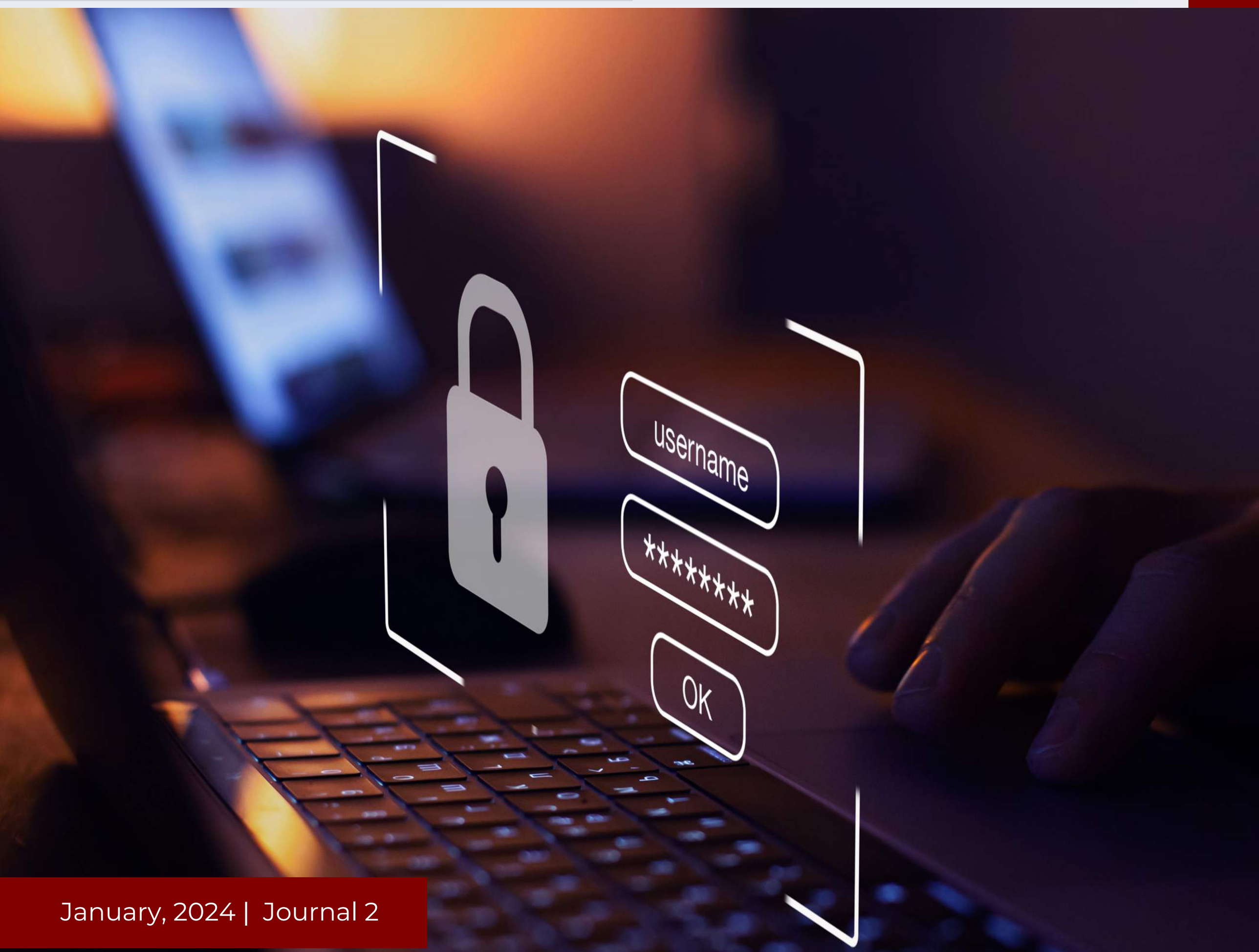
AMLEGALS
LEGAL STRATEGISTS

DATA PRIVACY
NEXT

DECODING DPDPA

INDIA



January, 2024 | Journal 2

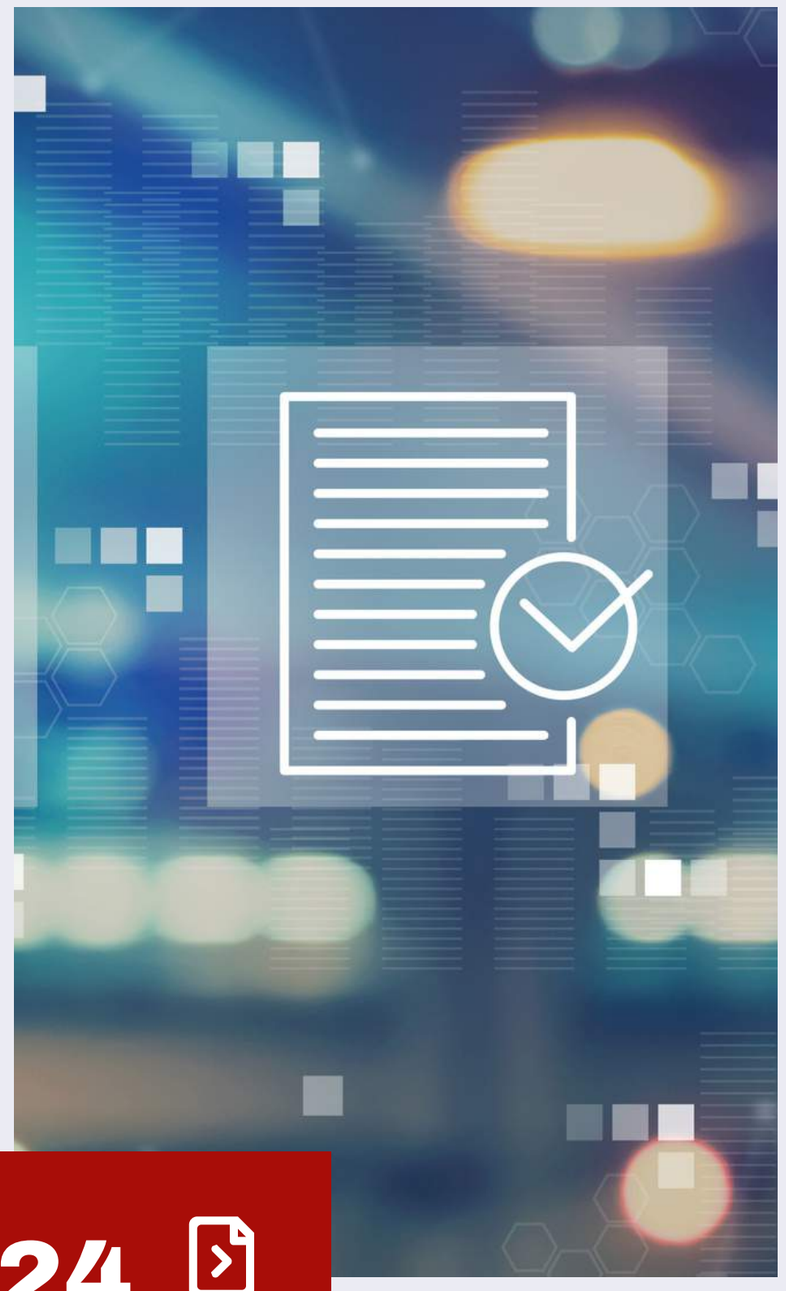
#RespectData

AHMEDABAD | BENGALURU | NEW DELHI | KOLKATA | HYDERABAD | MUMBAI | PUNE | SURAT

AMLEGALS
LEGAL STRATEGISTS

DATA PRIVACY NEXT

this is issue .in



Founder's Letter

With the introduction of the Digital Personal Data Protection Act, 2023, and the resulting strict compliance imposed upon the processing of data domestically and across jurisdictions, understanding the concept of Data Privacy is the need of the hour.

This is also the time when we can look at the global trends, and practical challenges pertaining to safeguarding personal data, faced by business entities in the wake of the era of big data.

Our data privacy and protection laws team entails a comprehensive and articulate understanding of the laws since 2018. Humbled with the 'Top Data Privacy Voice' badge on LinkedIn, I am personally a passionate enthusiast for Data Privacy laws, and it has always been our goal to share insights regarding every aspect of data privacy.

We at AMLEGALS are delighted to share the second edition of our Quarterly Journal on Data Protection, which will provide an overview into the different facets of the newly introduced Act.

We hope you find this resourceful.

Anandaday Misshra
Founder & Managing Partner | AMLEGALS

HOW TO CREATE A ROBUST DATA PROTECTION STRATEGY

INTRODUCTION

Implementing a robust data protection strategy in India, especially with the advent of the Digital Personal Data Protection Act, 2023 (**"DPDPA, 2023"**), would involve several key steps and considerations.

Here is a comprehensive approach to formulating an effective data protection strategy:

1. **Understand the DPDPA, 2023**
2. **Data Governance and Classification**
3. **Consent and Data Subject Rights**
4. **Data Protection Measures**
5. **Data Processing and Third-Party Management**
6. **Training and Awareness**
7. **Data Protection Impact Assessment**
8. **Legal and Regulatory Updates**
9. **Documentation and Record Keeping**
10. **Preparing for Audits and Certifications**
11. **Continuous Improvement**
12. **Additional Resources**

1. Understand the DPDPA, 2023

Key Provisions

Familiarize yourself with the basic and the main aspects of the DPDPA, 2023.

This includes understanding the rights of data principals, obligations of data fiduciaries, cross-border data transfer rules, and penalties for non-compliance, among other things.

Comparative Analysis

Compare the DPDPA with other global data protection laws like GDPR, CCPA, etc., to understand the similarities and differences.

This can help in creating a more globally compliant framework.

2. Data Governance and Classification

Data Inventory

Conduct a thorough data mapping exercise to identify what personal data is collected, processed, and stored.

Classification

Classify data based on various parameters in your organization. The classification can be based on collection, storage, retention pattern, access, business decisions, third party processing/access, etc.

This aids in applying appropriate security measures.

3. Consent and Data Subject Rights

Consent Mechanisms

Implement robust mechanisms for obtaining and recording consent from data subjects. Ensure the consent is given freely, is specific, informed, and unambiguous.

Rights of Individuals

Establish processes to facilitate data subjects' rights, like the right to access, rectification, data portability, and erasure.

4. Data Protection Measures

Technical Safeguards

Deploy appropriate security measures like encryption, anonymization, access controls, and regular security audits.

Policies and Procedures

Develop comprehensive data protection policies, including incident response plans and breach notification procedures.

5. Data Processing and Third-Party Management

The following would constitute the basis of data processing and third-party management under the DPDPA:

Data Processing Agreements

Ensure that contracts with third parties, i.e., data processors include clauses that mandate compliance with the DPDPA, 2023.

Third-Party Contracts

The third-party contracts such as the contracts with external vendors or agencies should be drafted crisply. Such contracts should be the topmost priority in any organization.

Vendor Assessment

Regularly assess third-party vendors for compliance with data protection standards.

6. Training and Awareness

Employee Training

Conduct regular training for employees on data protection best practices, legal requirements, and internal policies.

Red Flagging

Create a culture to focus on red flags including insider risks and involve stakeholders to fix it within a given deadline followed by a review.

Awareness Programs

Create awareness among stakeholders about the importance of data protection and the implications of the DPDPA, 2023.

7. Data Protection Impact Assessment (“DPIA”)

Conduct DPIAs

For new projects or data processing activities, assess the impact on personal data privacy and implement necessary controls.

Review DPIAs

Most organizations worldwide consider that DPIA is a one time work. However, on the contrary, it is a constant process.

8. Legal and Regulatory Updates

Staying Informed

Regularly update your knowledge on legal and regulatory changes in data protection, both in India and globally.

Compliance Reviews

Periodically review and update your data protection framework to ensure ongoing compliance.

9. Documentation and Record Keeping

Maintain Records

Keep detailed records of data processing activities, DPIAs, consent records, and data breaches.

Documentation

Ensure all data protection policies, procedures, and training materials are well documented and easily accessible.

Contracts/MOUs

Contracts/MOUs should be tailor-made and updated regularly.

10. Preparing for Audits and Certifications

Internal Audits

Regularly conduct internal audits to assess compliance with the DPDPA and other relevant regulations.

Review Mechanism

Set a regular review mechanism on audits and fix red flags highlighted during audits on top most priority.

Seek Certification

Consider obtaining certifications like ISO 27001 for information security management, which can bolster your organization's data protection posture.

11. Continuous Improvement

Feedback Loops

Establish mechanisms for receiving feedback and continuously improving data protection practices.

Benchmarking

Compare your practices with industry best practices and adjust as needed.

12. Additional Resources

Legal and Industry Reports

Stay updated with the latest research and reports from legal bodies, industry groups, and data protection authorities.

Checking Insider Risks

Conduct data protection workshops and implement robust practices as per your organisational need.

LEGAL STRATEGIES FOR COMPLIANCE WITH DPDPA, 2023

10 STRATEGIES

Compliance with the DPDPA, 2023, is not just a legal requirement but also a strategic necessity for organizations. Here is an in-depth look at various legal strategies for ensuring compliance with the DPDPA. 2023.

Risk Assessment & Gap Analysis

Objective: To identify areas where the organization is not in compliance with DPDPA, 2023.

Legal Strategy: Conduct a comprehensive audit of all data processing activities and map them against the requirements of the DPDPA. Identify gaps and potential risks.

Policy Development and Review

Objective: To develop internal policies that are compliant with the DPDPA.

Legal Strategy: Draft or revise Data Protection Policies, Privacy Policies, and other internal guidelines. Ensure that they are in line with the DPDPA and get them reviewed by legal experts.

Contractual Agreements

Objective: To ensure that all legal contracts are compliant with the DPDPA.

Legal Strategy: Revise existing contracts and draft new ones that include clauses mandating compliance with DPDPA, 2023. This is particularly important for contracts with data processors and third-party vendors.

Consent Mechanisms

Objective: To obtain lawful consent for data processing.

Legal Strategy: Draft clear and concise consent forms that meet DPDPA's requirements for explicit consent. Implement mechanisms for data subjects to easily withdraw consent.

Employee Training and Awareness

Objective: To ensure that all employees are aware of their responsibilities under the DPDPA.

Legal Strategy: Develop and implement a training program that educates employees on the DPDPA's provisions and the organization's data protection policies.

Appointment of Data Protection Officer (DPO)

Objective: To oversee data protection activities within the organization.

Legal Strategy: Appoint a DPO as mandated by the DPDPA. Ensure that the DPO has the necessary qualifications and independence to effectively carry out their role.

Data Protection Impact Assessments

Objective: To assess the impact of data processing activities on data subjects.

Legal Strategy: Establish a process for conducting DPIAs for new and existing data processing activities. Consult legal experts during the assessment.

Record-Keeping and Documentation

Objective: To maintain records of all data processing activities.

Legal Strategy: Implement robust documentation practices that record consent, DPIAs, audits, and data subject requests. This will be crucial for demonstrating compliance during audits or legal proceedings.

Incident Response Plan

Objective: To effectively respond to data breaches and other incidents.

Legal Strategy: Develop an incident response plan that outlines the steps to be taken in the event of a data breach, including notification to the Data Protection Authority and affected data subjects.

Regular Audits and Monitoring

Objective: To persistently assess compliance with the DPDPA.

Legal Strategy: Establish a schedule for regular internal and external audits. Engage legal experts to interpret audit findings and recommend corrective actions.

Every business entity is advised to take due diligence and opt for data protection expert advice to comply with the requirement under DPDPA, 2023.

DATA PROTECTION POLICY FOR COMPANIES IN INDIA

With the DPDPA, 2023 in place in India, the data protection regime is all set to begin and therefore, companies should work out their own Data Protection Policies so as to avoid the unforeseen liabilities.

Some suggestions to be included in the **Data Protection Policy** for your Business Organisations **in India**:

01 Organisation's General Approach

02 How Lawful Processing is being ensured

03 Compliance with Data Minimisation

04 Mechanism of Data Storage

05 Role of Data Protection Officer

06 Organisation's Review and Audit Process

07 Maintenance of Data Processing Records

08 Data Subject Rights

09 Data System Security Measures

10 Staff Training & Supervision Means

11 Data Processor Identity & Selection

12 Working of Consent Managers

13 Role & Duties of Data Fiduciary

14 Applicability of Policy to External Parties

15 Marketing and ePrivacy Aspects

16 Stringent Provisions for using Child Data

HOW TO CREATE A DATA PROTECTION POLICY

Creating a Data Protection Policy is a critical step for any business organisation that handles and process personal or sensitive information. A well-structured policy ensures that your organisation is fully compliant with data protection law in terms of the DPDPA, 2023.

The following steps can be adopted to create a robust Data Protection Policy:

Serial No.	Steps	Description
01	Understand Legal Requirements	Research applicable data protection laws and regulations relevant to your jurisdiction and make a checklist of the compliance requirements.
02	Appoint a Data Protection Officer	Choose a competent individual responsible for data protection compliance.
03	Identify the Scope	Define who the policy will affect: employees, contractors, partners, customers, etc.
04	Conduct a Data Audit	Inventory what types of data you collect, where it’s coming from, how it’s used, and where it’s stored.
05	Define Key Principles	Your policy should reflect the key principles of data protection: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.
06	Data Collection	Describe the types of data you collect and the legal basis for processing this data.
07	Data Usage	Clearly define the purpose for data collection and processing.

Serial No.	Steps	Description
08	Data Storage	Outline how and where the data will be securely stored.
09	Data Sharing and Transfers	Explain if, how, and why data might be shared with third parties.
10	Data Subject Rights	Describe the rights of data subjects under relevant data protection laws.
11	Data Breach Procedure	Create a procedure for notifying authorities and data subjects in case of a data breach.
12	Dos and Don’ts	Outline the best practices and things to avoid in data handling within the organisation.
13	Policy Review and Updates	Indicate how often the policy will be reviewed and updated.
14	Approvals	Get approval from higher management or the board, as appropriate.
15	Policy Distribution	Make sure all stakeholders, including employees and contractors, are aware of and understand the policy.

By following the aforesaid steps, any organisation can create a comprehensive Data Protection Policy that ensures the organisation’s compliance with data protection laws in India.

AGREEMENTS

ESSENTIAL FOR DATA PROTECTION

10 AGREEMENTS

Different types of Agreements which are essential for data protection in the context of stringent regulations of the DPDPA, 2023 are as under:

Data Processing Agreement

Purpose: To outline the terms under which data will be processed by a data processor on behalf of a data controller.

Key Clauses: Scope of processing, data subject rights, security measures, sub-processors, and audit rights.

Example: A cloud service provider entering into a DPA with a corporate client to store employee data.

Data Sharing Agreement

Purpose: To govern the sharing of data between two or more parties.

Key Clauses: Types of data to be shared, purpose of sharing, security measures, and data retention policies.

Example: Two healthcare providers sharing patient's data for research purposes.

Non-Disclosure Agreement

Purpose: To protect confidential information, including personal data, that may be disclosed during business operations.

Key Clauses: Definition of confidential information, obligations of the parties, and penalties for breach.

Example: A software development company entering into an NDA with a freelance developer.

Service Level Agreement

Purpose: To specify the level of service expected from a data processor, including data protection standards.

Key Clauses: Performance metrics, security standards, and remedies for non-compliance.

Example: An e-commerce platform and a payment gateway provider.

Data Protection Addendum

Purpose: To add data protection clauses to an existing contract that may not adequately address data protection.

Key Clauses: Data protection responsibilities, compliance with laws, and indemnification.

Example: Companies modifying their existing Employment Agreements *vide* an Addendum.

Consent Agreement

Purpose: To obtain explicit consent from data subjects for data collection and processing.

Key Clauses: Scope of consent, withdrawal mechanism, and data subject rights.

Example: A medical research organization obtaining consent from participants.

End-User License Agreement

Purpose: To define the terms under which end-users can use a software or application, including how their data will be handled.

Key Elements: Data collection, usage, third-party sharing, and data protection measures.

Example: A mobile app providing its services to consumers.

Cloud Service Agreement

Purpose: To outline the terms under which data will be stored and processed in a cloud environment.

Key Clauses: Data ownership, security measures, and data transfer protocols.

Example : The agreement to define the terms and conditions under which the client's data will be stored, processed, and secured in the cloud environment provided by the Cloud Service Provider.

Joint Controller Agreement

Purpose: To specify the responsibilities of each party when two or more entities act as joint controllers of personal data.

Key Clauses: Allocation of responsibilities, data subject rights, and dispute resolution mechanisms.

Example : Entity A shall be responsible for obtaining consent from data subjects, while Entity B shall be responsible for securely storing and processing the data

Data Retention Policy /Agreement

Purpose: To specify how long data will be retained and the procedures for data deletion.

Key Clauses: Data categories, retention periods, and deletion procedures.

Example: Personal data will be retained for 5 years, financial data for 7 years, and health records will be retained indefinitely unless otherwise required by law.

The above stated are few of the contracts and agreements which is the legal backbone of any data protection strategy. These agreements should define the roles, responsibilities, and liabilities of all parties involved in the processing of personal data. Given the stringent requirements and potential penalties under DPDPA, 2023, having well-drafted contracts is not just advisable but essential for compliance.

Each type of agreement serves a specific purpose and requires a deep understanding of both legal and technical aspects to ensure robust data protection. Your role in drafting, reviewing, and advising on these contracts will be pivotal in navigating the complex landscape of data protection law in India.

DATA PROTECTION IMPACT ASSESSMENT UNDER DATA PRIVACY ERA

DATA PROTECTION IMPACT ASSESSMENT

DPIA is a procedure wherein an evaluation is conducted to comprehend the potential risks which are likely to come in way while personal data is processed.

DPIA sets up the way forward to reduce the risk associated with the data processing as much as possible.

All kinds of organizations – whether Micro, Small, and Medium Enterprises (**"MSMEs"**), or multinational conglomerates are advised to initiate the process of DPIA.

The process of DPIA into the data management system of the companies is one of the critical prerequisites to comply with the requirement of DPDA, 2023.

It is significant to understand this aspect in line with the following questions discussed moving forward.

WHETHER DPIA IS MANDATORY?

It is pertinent to note that as per clause (c) of Section 10 (2) of the DPDPA, 2023, the Significant Data Fiduciary shall undertake the DPIA, which shall be a process comprising of the following:

- description of the rights of Data Principals,
- purpose of processing of their personal data,
- assessment and management of the risk to the rights of the Data Principals, and
- such other matters regarding such process as may be prescribed under DPDPA, 2023.

Yes, it can be safely concluded that DPIA is a mandatory exercise to be carried out by every Significant Data Fiduciary under the enactment.

WHEN TO CARRY OUT DPIA?

It should be carried out before carrying out any data processing project.

WHETHER A SEPARATE DPIA IS TO BE CARRIED TOWARDS EACH PROJECT?

Yes, since every project and assessment can have varied factors to be assessed.

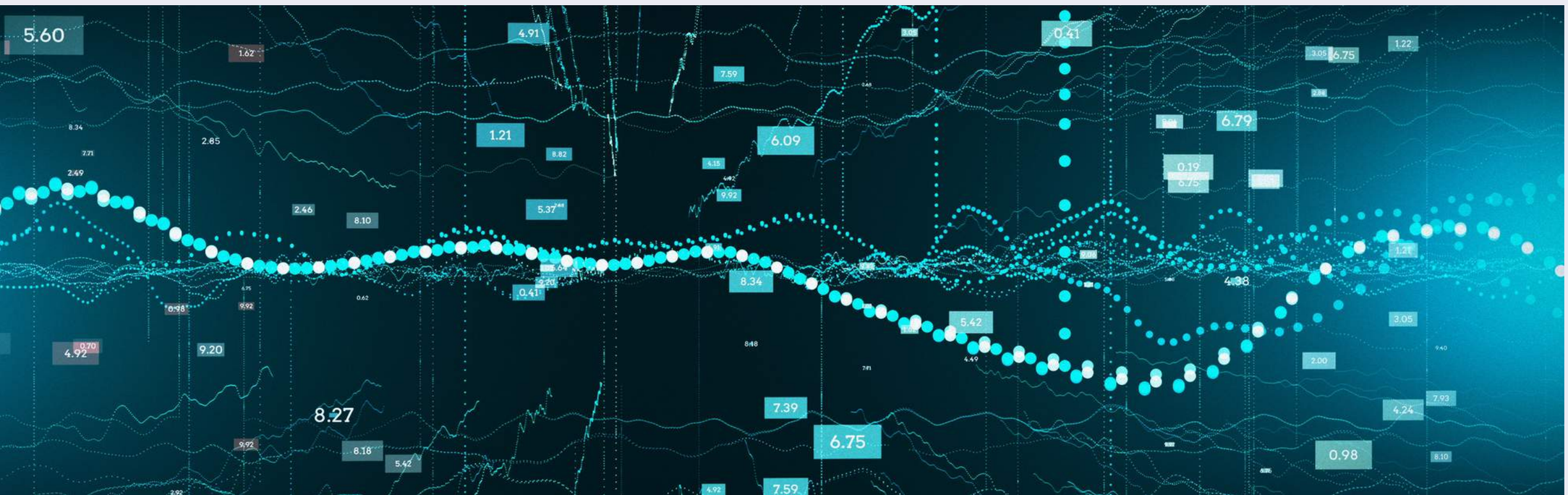
WHAT ARE THE BROADER HEADS OF RISKS TO BE ASSESSED?

The risks should be broadly classified under:

1. Associated with Data Principals
2. Corporate risks, and
3. Compliance risks

WHETHER DPIA SHOULD BE PUBLISHED?

Yes, it should be published as then only you can have everything documented and specified along with the rights of Data Principals, process to be carried out and risk assessed and should be duly taking a note of a project with number, date and description.



FACTSHEET IN DATA PROTECTION IMPACT ASSESSMENT

A factsheet in a DPIA serves as a comprehensive summary or overview of the assessment. It is essentially a distilled version of the DPIA that quickly highlights the key points, such as the data being collected, the purpose for the collection, potential risks, and mitigations.

The factsheet is generally intended for a varied audience that can range from stakeholders and decision-makers to the general public. Therefore, it should be easily understandable without sacrificing the necessary detail.

The key components of a DPIA Factsheet are as under:

01 Project Name and Description

02 Information about Data Controller

03 Purpose of Data Collection

04 Data Categories

05 Data Sources

06 Data Processing Activities

07 Data Recipients

08 Risk Assessment

09 Mitigation Measures

10 Legal Compliance

11. Contact Information

10 STRATEGIES FOR A COMPREHENSIVE FACTSHEET

The preparation of the factsheet is very crucial for proper DPIA in any organisation. The important factors to be considered are as below:

01 Gather Information

Before creating a factsheet, make sure you have all the information gathered from the DPIA process. The factsheet will be a summary of this information.

02 Understand the Audience

Tailor the language and content based on who will be reading the factsheet.

03 Use a Clear Structure

Use headings, bullet points, and numbers to make it easy to read and understand.

04 Be Concise but Detailed

Provide enough detail to give a comprehensive overview but be as concise as possible to make it easy to understand.

05 Use Plain Language

Avoid jargon or technical terms that could confuse non-experts.

06 Review for Accuracy

Make sure all information is accurate and up-to-date. Any mistakes can undermine the trustworthiness of the DPIA and may have legal implications.

07 Get Feedback

Before finalising, seek feedback from stakeholders or experts to make sure the factsheet accomplishes its goal of effectively summarising the DPIA.

08 Update Regularly

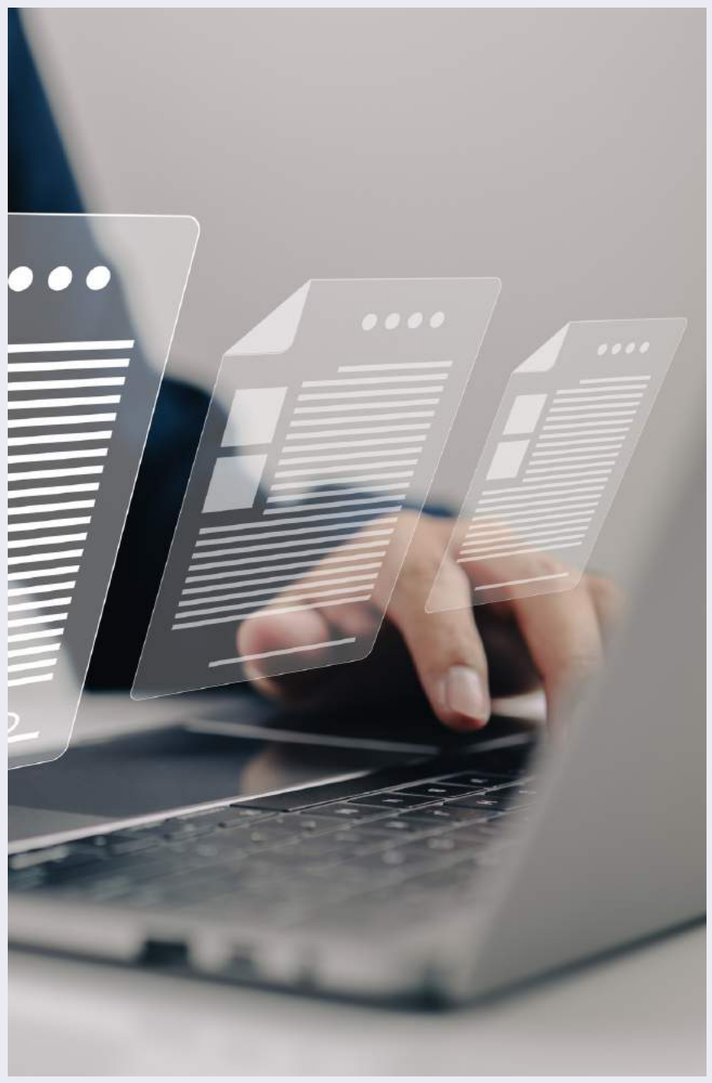
Any changes to the DPIA should be reflected in the factsheet. Make sure it is kept up-to-date.

09 Make it Accessible

The factsheet should be easily accessible, whether that means being downloadable from a website or available in paper form.

10 Legal Review

Depending on the complexity and risk associated with the project, consider having the factsheet reviewed by legal experts to ensure compliance with relevant laws and regulations.



AT A GLANCE

The data protection era in India reflects a growing awareness of the need to safeguard individuals' privacy in the digital age. India's approach to data protection aligns with global trends, particularly in light of regulations like the GDPR in the European Union. The increasing focus on data protection is essential not only for safeguarding individual privacy but also for fostering trust in digital services and cross-border data flows.

The effectiveness of the data protection era in India will depend on the successful implementation of the provisions of the DPDPA, 2023, the establishment of the regulatory bodies, and ongoing efforts to adapt to evolving technological landscapes. Additionally, fostering a culture of data privacy awareness among businesses and individuals will be crucial for the long-term success of data protection measures.

DATA PROTECTION TEAM

Anandaday Misshra
Founder & Managing Partner

Ajay Goyal
Sr. Advisor

Rohit Lalwani
Associate Partner

Mridusha Guha
Senior Associate

Himanshi Patwa
Associate

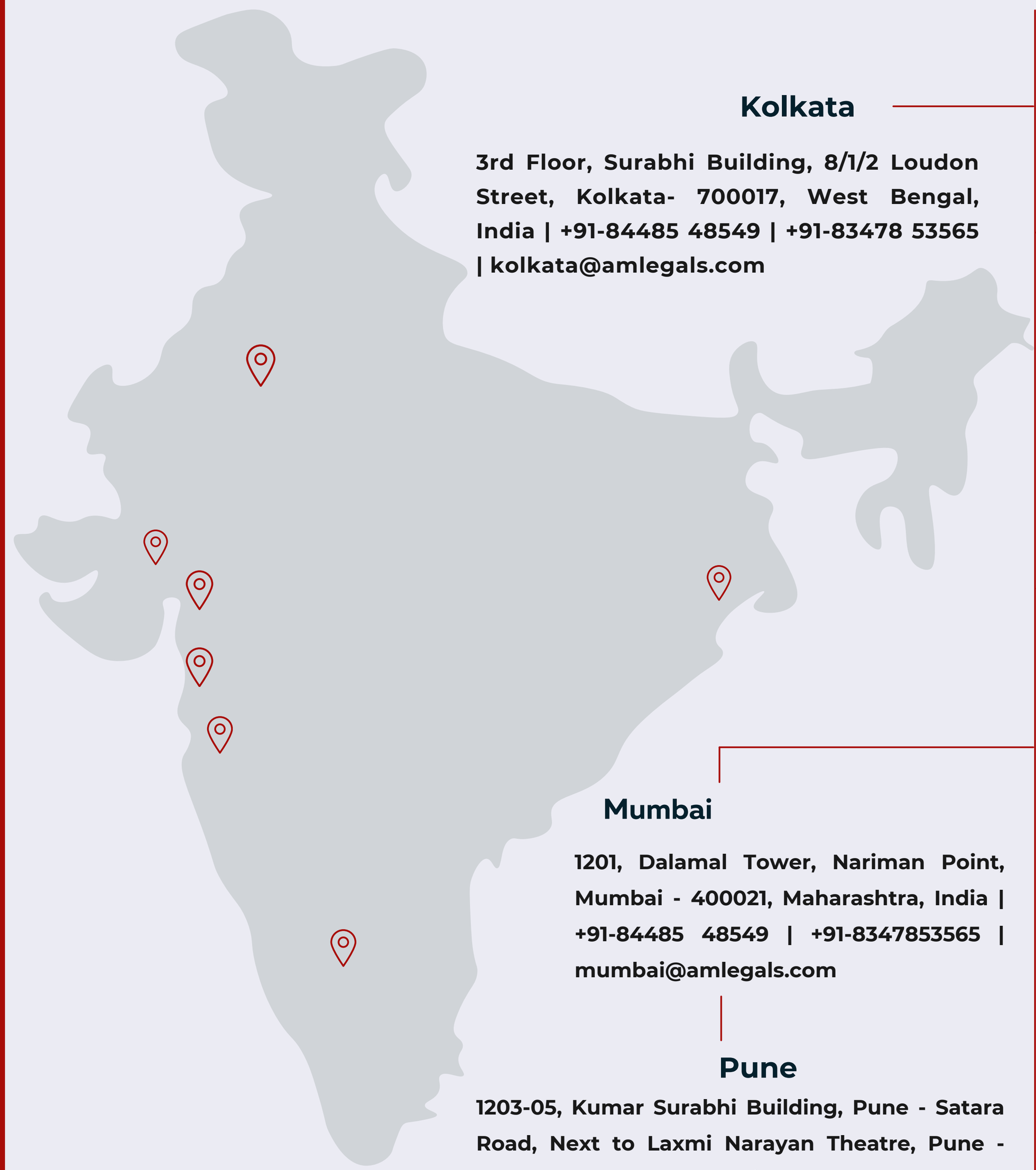
Liza Vanjani
Associate

Jason James
Associate

AMLEGALS
LEGAL STRATEGISTS

DATA PRIVACY NEXT

India Offices



AHMEDABAD (H.O.)

201-203, AMLEGALS, Westface, Near. Baghban Part Plot, Zydus Hospital Road, Thaltej - 380059, Ahmedabad
+91-84485 48549 | +91-8347853565

Kolkata

3rd Floor, Surabhi Building, 8/1/2 Loudon Street, Kolkata- 700017, West Bengal, India | +91-84485 48549 | +91-83478 53565 | kolkata@amlegals.com

Surat

B-502, Shreeji Arcade, Anand Mahal Road, Adajan, Surat | 84485-48549 | 83478-53565 | surat@amlegals.com

Gurgaon

RMZ Infinity, Udyog Vihar Phase – IV, Gurgaon - 122001, India | +91-84485 48549 | +91-8347853565 | gurgaon@amlegals.com

Mumbai

1201, Dalamal Tower, Nariman Point, Mumbai - 400021, Maharashtra, India | +91-84485 48549 | +91-8347853565 | mumbai@amlegals.com

Pune

1203-05, Kumar Surabhi Building, Pune - Satara Road, Next to Laxmi Narayan Theatre, Pune - 411009, Maharashtra, India | +91-84485 48549 | +91-8347853565 | pune@amlegals.com

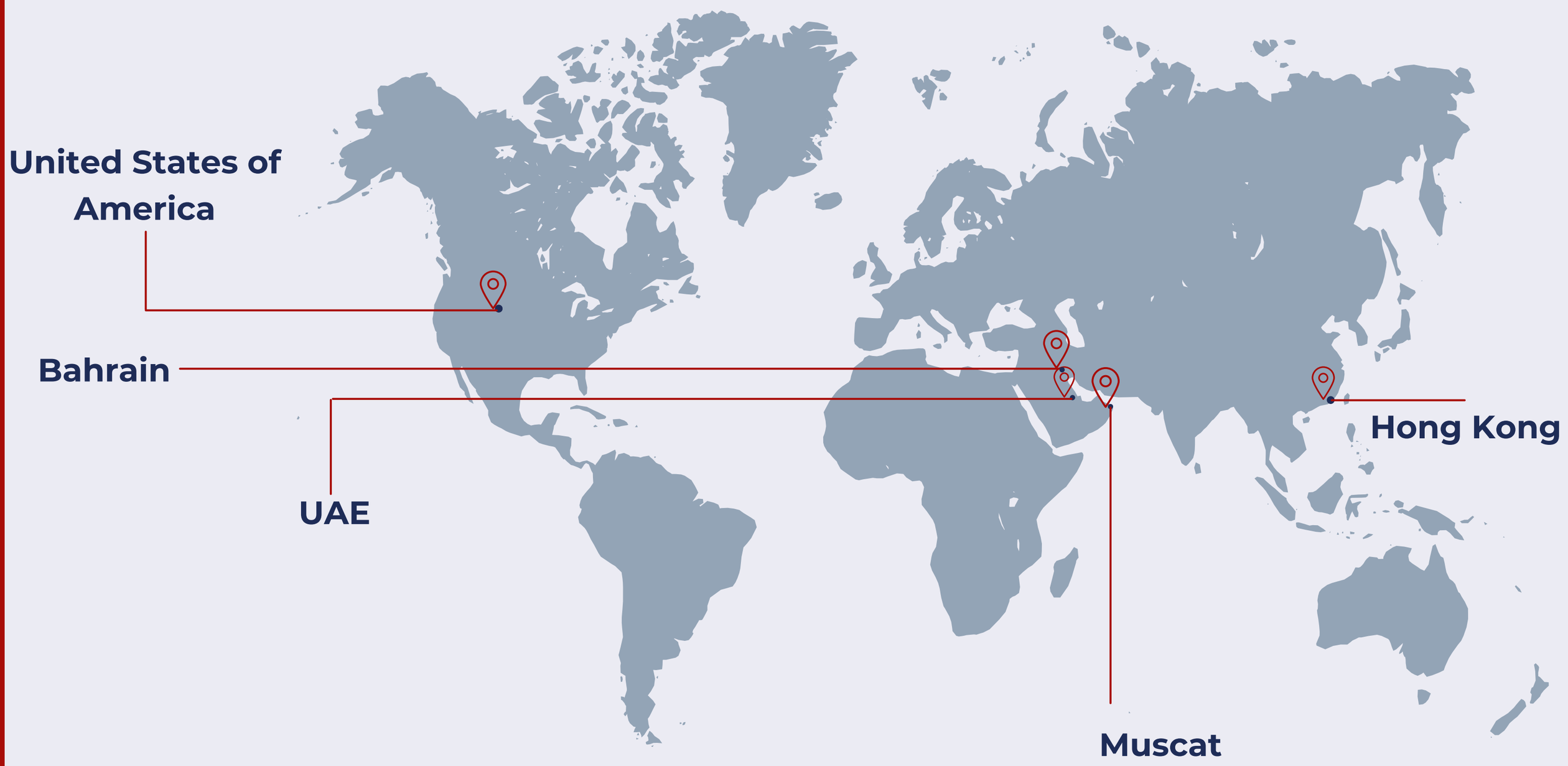
Bengaluru

CoWrks NXT, Block 1B, RMZ NXT, EPIP, Whitefield Main Rd, Industrial Area, Bengaluru - 560066, Karnataka, India | +91-84485 48549 | +91-83478 53565 | bengaluru@amlegals.com

AMLEGALS
LEGAL STRATEGISTS

DATA PRIVACY
NEXT

International Desks



International Associates

E-mail

dataprivacy@amlegals.com

Website

www.amlegals.com

AMLEGALS
LEGAL STRATEGISTS