jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection

Digital Personal Data Protection Act

Edition IV

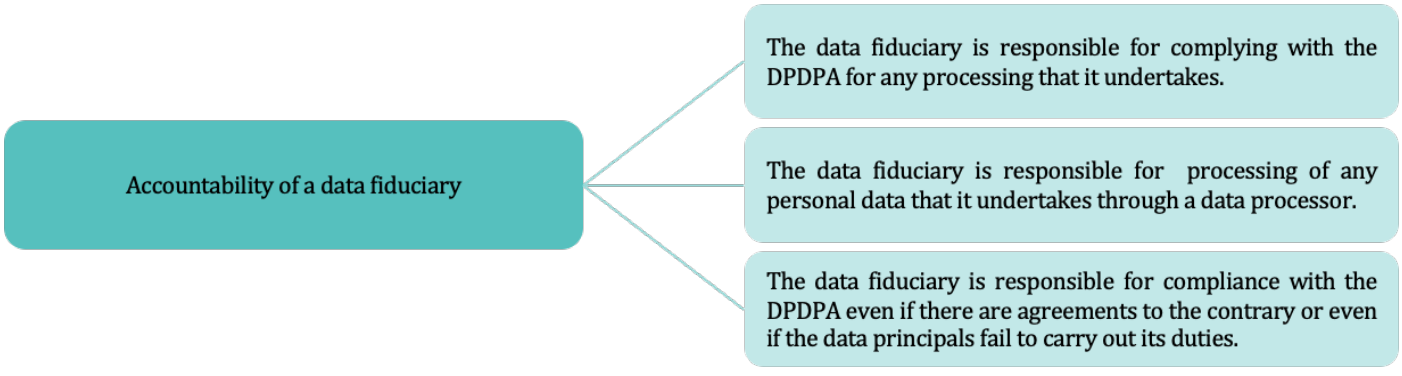
August 2024

General obligations of data fiduciaries and significant data fiduciaries

In the fourth instalment of the Prism series on the Digital Personal Data Protection Act, 2023 ("**DPDPA**"), we analyse the general obligations of data fiduciaries and Significant Data Fiduciaries ("**SDF**s"). These obligations encompass principles like accountability, fairness, storage limitation, preserving the integrity and confidentiality of personal data, etc. In the latter part of the Prism, we compare these obligations with data protection laws around the world to identify obligations of data fiduciaries under the General Data Protection Regulation ("**GDPR**"), California Consumers Privacy Act ("**CCPA**") and the Singapore's Personal Data Protection Act ("**PDPA**").

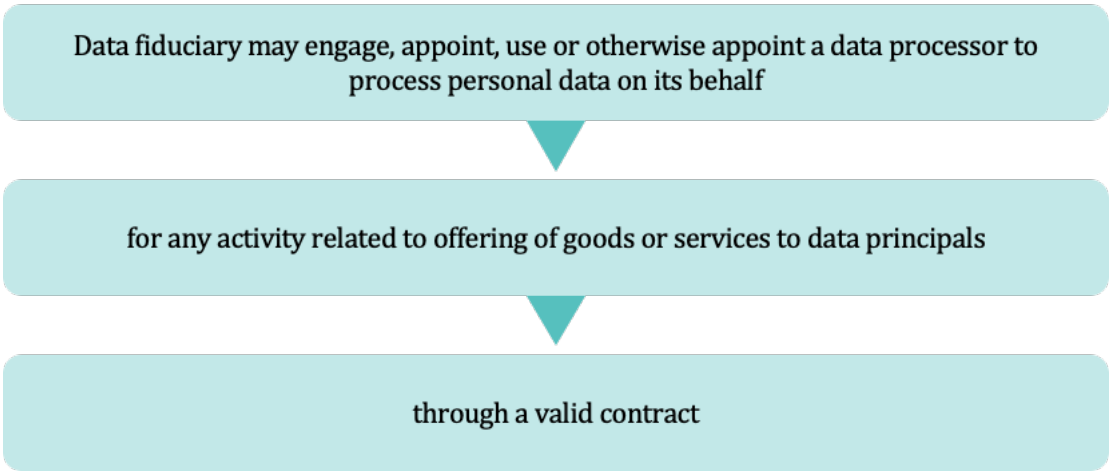
What are the obligations of a data fiduciary?

1. **Accountability:**

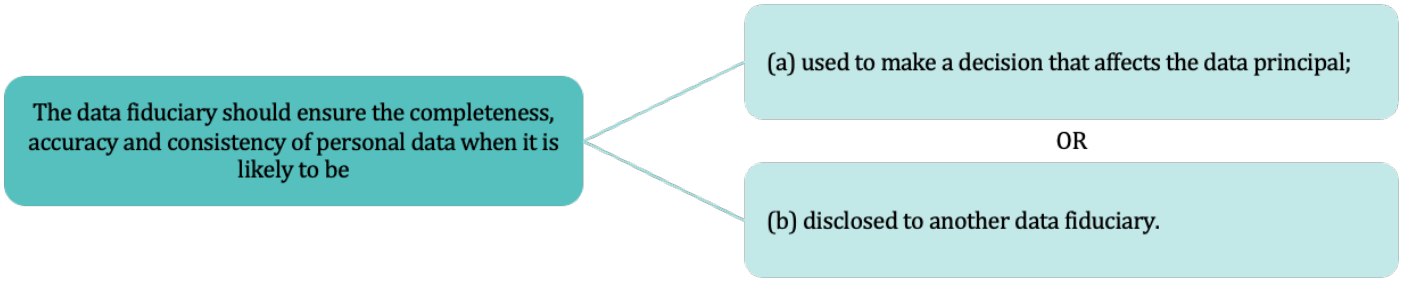


- Data processors are defined under the DPDPA to mean any person who processes personal data on behalf of a data fiduciary.
- It is pertinent to note that unlike the GDPR the data processors do not have any direct obligations under the DPDPA. The data fiduciary is responsible for the compliance of the data processors. Therefore it is important to undertake due diligence on data processors before their appointment.
- The DPDPA does not mandate maintaining a record of processing activities ("**ROPA**"). However maintaining a ROPA will help in identifying gaps in compliance with the DPDPA, and it will also help in responding to data principals' access rights.
- The GDPR mentions that a controller can demonstrate compliance with the GDPR by implementing internal data protection policies, by adhering to code of conduct or certification mechanism. However, the DPDPA does not explicitly mention any measures by which data fiduciary can demonstrate compliance with its obligations.

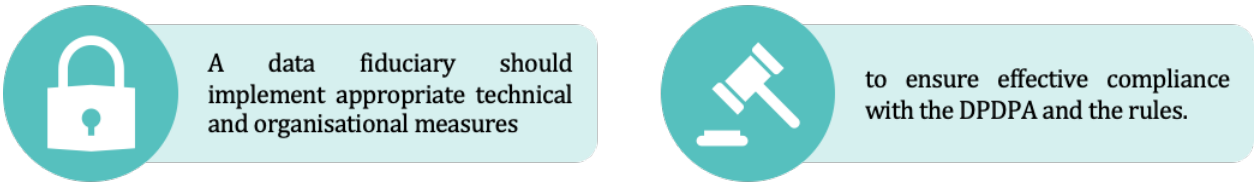
2. **Engagement of data processors:**



3. **Ensuring completeness, accuracy and consistency of personal data:**



4. **Implementing technical and organizational measures:**



- The GDPR mentions implementing privacy by design and default and other measures like pseudonymising personal data or encryption of personal data as an example of implementing measures to meet the principles of data protection. However, the DPDPA does not elaborate upon the technical and organisational measures for compliance with the DPDPA.
- The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 state that body corporates which have implemented the international standard IS/ISO/IEC 27001 or followed data protection best practice codes provided by an association are deemed to have complied with reasonable security practices and procedures. However, the DPDPA does not provide any such standards for demonstrating compliance.

5. **Protection of personal data:**

The data fiduciary should protect personal data in its possession or under its control by implementing measures. ▶ The measures may include directing the data processors to take reasonable security safeguards to prevent personal data breach.

6. **Intimation of personal data breach:**

In the event of a personal data breach, the data fiduciary should
- (a) notify the Data Protection Board
  (The Rules will prescribe the form and manner to notify the board).
- (b) notify the affected data principals.

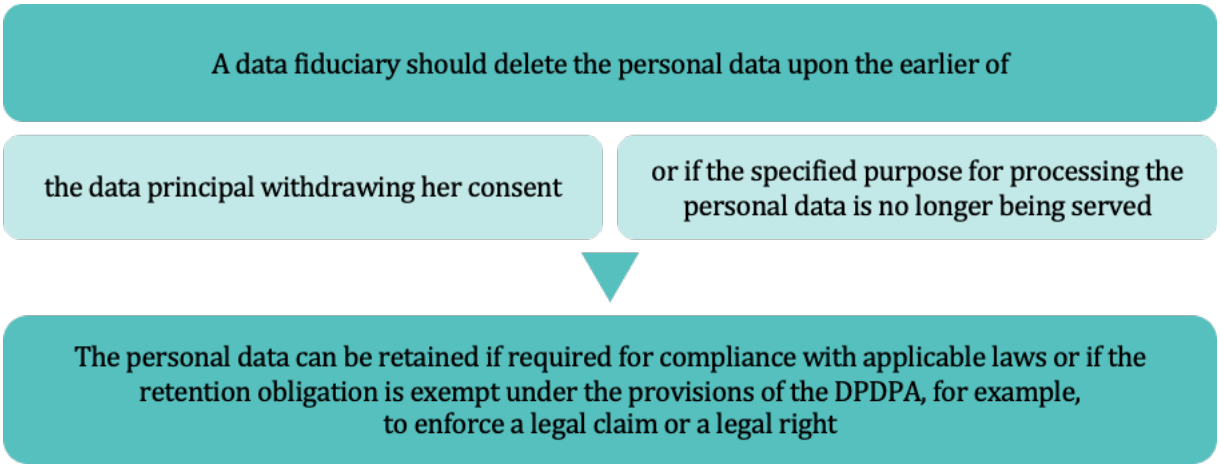
7. **Contact details of the Data Protection Officer ("DPO") or authorized person of the data fiduciary:**

The data fiduciary should publish:
- (a) The contact details of the DPO if applicable
  (The rules will mention the manner of publishing the business contact information of a DPO.)
- (b) If appointment of a DPO is not applicable, then the details of the personnel who can answer the questions raised by the data principal on behalf of the data fiduciary.

8. **Effective grievance redressal mechanism:**

Data fiduciaries should establish an effective mechanism to redress the grievances of data principals.

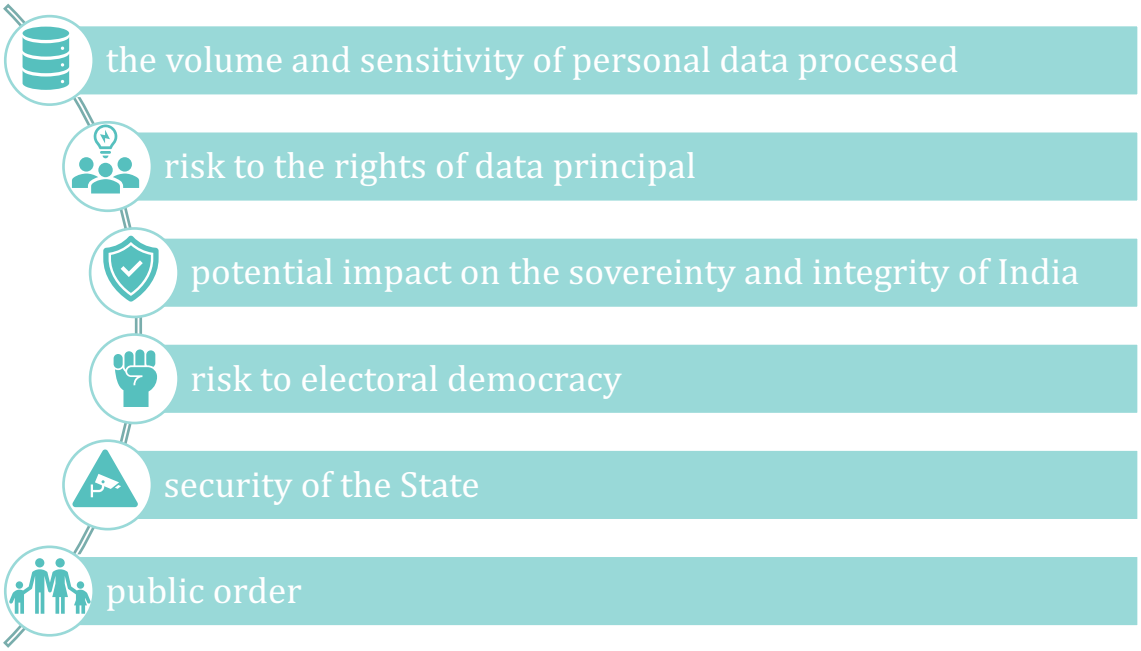
9. **Retention of personal data:**



The specified purpose will be deemed to be no longer served if within a time period, the data principal does not approach the data fiduciary for the purpose or to exercise any of her rights. The time period will be mentioned in the rules.

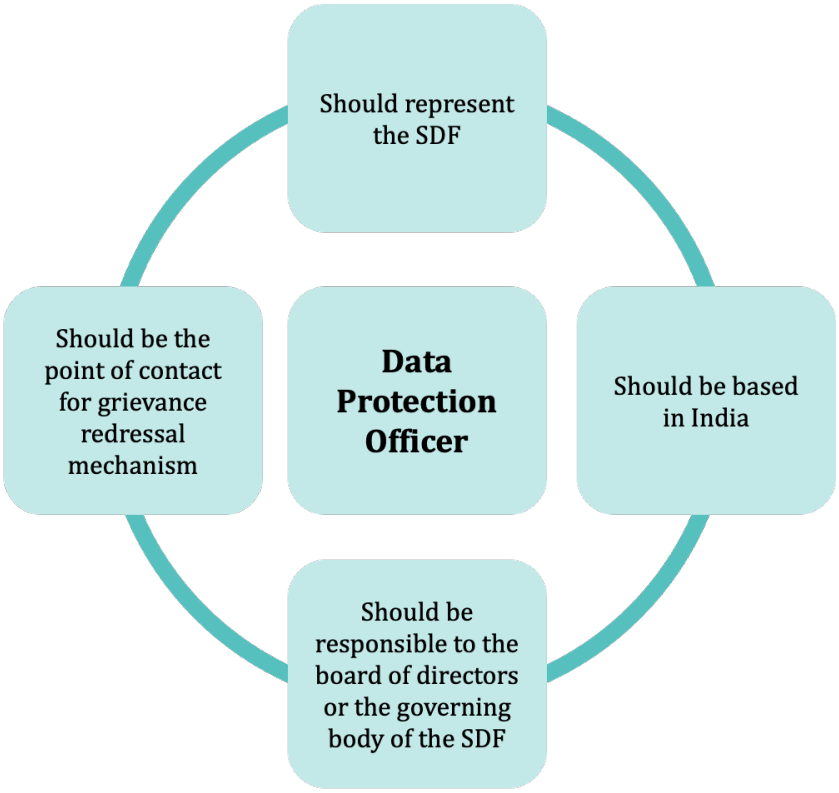
Who are SDFs?

SDF means any data fiduciary or class of data fiduciaries as the Central Government may notify from time to time based on assessment of certain factors that are captured below.



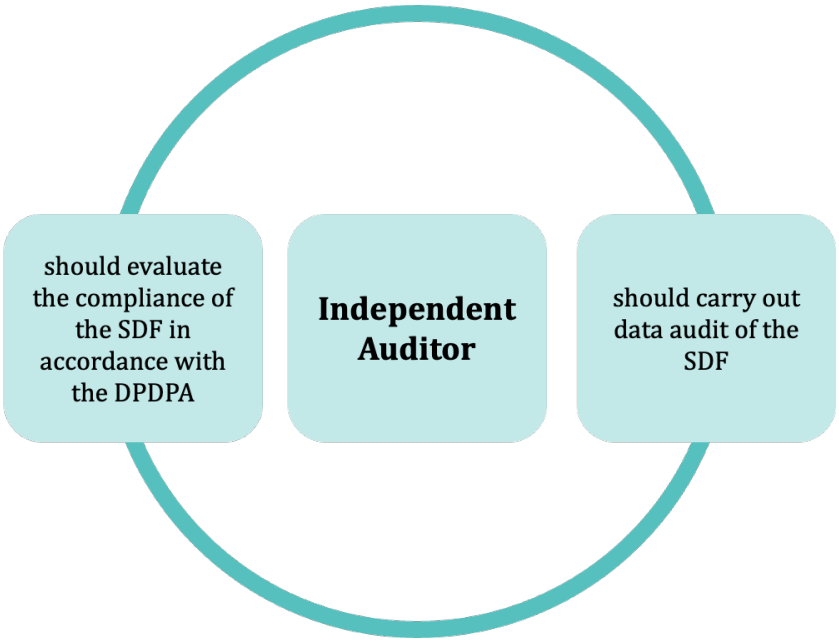
An SDF has certain obligations, in addition to the general obligations of a data fiduciary, listed below:

1. **DPO:** An SDF should appoint a DPO.

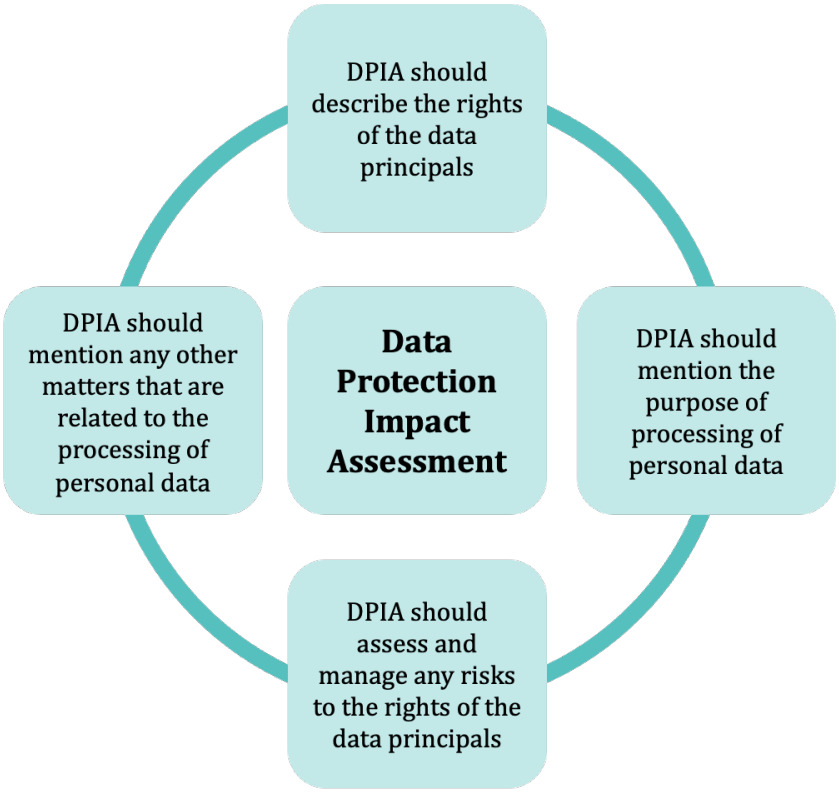


Although the DPDPA does not require the appointment of a representative, the SDFs are required to appoint a DPO who is based in India. However, for other data fiduciaries who are not classified as an SDF, there is no requirement to appoint a DPO or representative who is based out of India.

2. **Independent Auditor:** An SDF should appoint an independent auditor.



3. **Data Protection Impact Assessment:** An SDF should undertake periodic Data protection Impact Assessment ("DPIA").



The rules will mention the other matters that are related to the processing of personal data that should be part of the DPIA.

4. **Periodic Audit:** An SDF should also undertake periodic audit of its personal data processing activities
5. **Other measures:** An SDF should also undertake other measures that are consistent with the DPDPA. *The rules will mention more measures that an SDF will have to undertake.*

Comparison with select data protection laws around the world

Concept	DPDPA	GDPR	CCPA	PDPA
Implementation of technical and organisational measures	A data fiduciary should implement appropriate technical and organizational measures to comply with DPDPA.	The data controller should implement appropriate technical and organisational measures to comply with GDPR.	A business should implement reasonable security procedures and practices appropriate for the processing of personal information.	An organisation must develop and implement policies and practices to meet the obligations under PDPA.
Appointment of sub-processors	The data fiduciary can appoint a sub-processor through a valid contract.	The controller can appoint processors through a binding written contract.	A business can appoint a service provider for a business purpose pursuant to a business contract.	An organisation can appoint data intermediaries pursuant to a written contract.

Personal Data breach notification	The data fiduciary will notify the board and the affected data principals in case of a personal data breach.	The controller without undue delay and within 72 hours of becoming aware of a personal data breach, notify the supervisory authority and the data subject without undue delay unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	The California's breach notification statute mandates that consumers should be notified of data breach without unreasonable delay. The business must notify the attorney general if more than 500 consumers' personal information has been breached.	If the data breach is a notifiable data breach, the organisation will have to notify the commission within 3 days from the date of the assessment. The organisation should also notify the affected data subjects.
DPIA	The requirement to undertake a DPIA is only imposed on an SDF.	The controller, prior to the processing, carry out a DPIA where the processing is likely to result in a high risk to the rights and freedoms of natural persons.	Businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security will conduct a risk assessment.	Where an organisation processes personal data based on deemed consent, it will conduct an assessment.
Designation of the DPO	An SDF is obligated to appoint DPO.	The controller may appoint a DPO if its core activities require large-scale, regular processing and systematic monitoring of individuals or consist of large-scale processing of special categories of data.	The CCPA does not obligate the appointment of a DPO.	The organisation must designate an individual to ensure that the organisation complies with the PDPA.
Grievance redressal	Data fiduciaries will establish an effective mechanism to redress the grievances of data principals.	There is no obligation on the controller to provide an internal grievance redressal mechanism under the GDPR.	There is no obligation on the business to provide grievance redressal mechanism under the CCPA.	An organisation should develop a process to receive and respond to complaints that may arise with respect to the application of PDPA.
Retention of personal data	The data fiduciary should erase personal data if the data principal has withdrawn their consent or if the purpose is no longer being served	One of the principles of the GDPR ("storage limitation") mandates that the personal data should not be retained for longer than what is necessary to achieve the purpose of processing.	A business's retention of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.	Organisations should delete personal data as soon as the purpose for which the personal data was collected is no longer being served or if the retention is no longer necessary for legal or business purposes.

Obligation to ensure personal data's completeness, accuracy and consistency	Where the personal data is likely to be used to make a decision that affects the data principal or will be disclosed to another data fiduciary, then the data fiduciary shall ensure its completeness, accuracy and consistency.	One of the principles of data protection is to ensure that the personal data is accurate and, where necessary, kept up to date; if personal data is inaccurate, it should be rectified without delay.	The business has an obligation under the CCPA to entertain consumer requests to correct any inaccuracies in the personal information.	The organisation must take reasonable efforts to ensure that the personal data is accurate and complete where the personal data is likely to be used to make a decision that affects the data subjects or if likely to be disclosed by the organisation to another organisation.
Data audit	DPDPA mandates SDFs to conduct a data audit by an independent auditor.	GDPR does not mandate any data audit by an independent auditor.	CCPA directs the California privacy protection agency to make rules requiring businesses to do annual independent cybersecurity audits if the processing presents significant risk to consumers' privacy or security.	PDPA does not mandate any data audit by an independent auditor.

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

[Akshaya Suresh](#)
Partner

[Aravindini Magesh](#)
Associate

Chambers TOP RANKED Asia-Pacific 2024 JSA

18 Practices and
25 Ranked Lawyers

Chambers TOP RANKED Global 2024

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice
---
3 Band 1 Practices
---
4 Band 1 Lawyers,1 Eminent Practitioner

IFLR 1000 TOP TIER FIRM 2023

12 Practices and
42 Ranked Partners
IFLR1000 APAC Rankings 2023

Banking & Finance Team of the Year

Fintech Team of the Year

Restructuring & Insolvency Team of the Year

The Legal 500

14 Practices and
38 Ranked Lawyers

asialaw OUTSTANDING FIRM 2024

20 Practices and
22 Ranked Lawyers

The Legal 500

Ranked Among Top 5 Law Firms in India for ESG Practice

GCR 100 2024

Recognised in World's 100 best competition practices of 2024

Among Top 7 Best Overall Law Firms in India and 11 Ranked Practices

---

11 winning Deals in IBLJ Deals of the Year

---

12 A List Lawyers in IBLJ Top 100 Lawyer List

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services Law Firm of the Year 2022

Ranked #1
The Vahura Best Law Firms to Work Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

www.jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi