

Privacy Policy — DPDP Act 2023 (India)

Compliant Privacy Policy for Indian startups under the Digital Personal Data Protection Act 2023

HOW TO USE THIS TEMPLATE

1. This Privacy Policy must be published on your website alongside your Terms of Service.
2. The Digital Personal Data Protection Act 2023 (DPDP Act) is now in force — compliance is mandatory.
3. Review and update whenever you change how you collect, use, or share personal data.
4. Translate the published version into Hindi and other Indian languages if your users include non-English speakers.
5. Designate a Data Protection Officer (DPO) or Grievance Officer as required under the DPDP Act.

COMPANY AND DATA CONTROLLER DETAILS

Data Fiduciary (Controller) Name	[Company full legal name]
CIN	[CIN]
Registered Address	[Registered office address with PIN code]
Data Protection Officer / Grievance Officer	[Name, email, and phone of designated DPO or GO]
Privacy Contact Email	[privacy@yourcompany.com]
Website	[https://www.yourwebsite.com]
Date of Last Update	[DD Month YYYY]
Applicable Law	Digital Personal Data Protection Act 2023 (DPDP Act); Information Technology Act 2000; IT (Reasonable Security Practices) Rules 2011

1. INTRODUCTION AND SCOPE

1.1 [Company Name] (the "**Company**", "**we**", "**us**", or "**our**") is committed to protecting the personal data of all individuals who interact with our Platform. This Privacy Policy explains how we collect, use, store, share, and protect your personal data in accordance with the Digital Personal Data Protection Act 2023 ("**DPDP Act**") and applicable rules.

1.2 This Policy applies to: (a) users of our website and mobile application; (b) customers who subscribe to our paid services; (c) visitors to our website; and (d) individuals whose personal data we receive through our business operations, including employees, contractors, and business partners. For employee data processing, a separate Employee Data Privacy Notice is provided at onboarding.

2. PERSONAL DATA WE COLLECT

2.1 Data You Provide Directly:

<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'Category' frags: [ParaFrag(tag='b', bold=1, fontName='Helvetica-Bold', fontSize=8, greek=0, italic=0, link=[], rise=0, text='Category', textColor=Color(.266667,.266667,.266667,1), us_lines=[])] style: 'bulletText': None 'debug': 0) #Paragraph</pre>	<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'Specific Data Points' frags: [ParaFrag(tag='b', bold=1, fontName='Helvetica-Bold', fontSize=8, greek=0, italic=0, link=[], rise=0, text='Specific Data Points', textColor=Color(.266667,.266667,.266667,1), us_lines=[])] style: 'bulletText': None 'debug': 0) #Paragraph</pre>	<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'When Collected' frags: [ParaFrag(tag='b', bold=1, fontName='Helvetica-Bold', fontSize=8, greek=0, italic=0, link=[], rise=0, text='When Collected', textColor=Color(.266667,.266667,.266667,1), us_lines=[])] style: 'bulletText': None 'debug': 0) #Paragraph</pre>
Account data	Name, email, phone number, password, profile photo	Account registration
Identity verification	PAN, Aadhaar (last 4 digits), GST number (for business accounts)	KYC process
Payment data	Card details (not stored by us — processed by payment gateway), billing address, GSTIN	Purchase / subscription
Communication data	Support tickets, emails, chat messages, feedback forms	When you contact us
User Content	Data, files, and information you upload or input into the Platform	During platform use
Business data	Company name, designation, team details	Business account setup

2.2 Data Collected Automatically:

<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'Category' frags: [ParaFrag(tag='b', bold=1, fontName='Helvetica-Bold', fontSize=8, greek=0, italic=0, link=[], rise=0, text='Category', textColor=Color(.266667,.266667,.266667,1), us_lines=[])] style: 'bulletText': None 'debug': 0) #Paragraph</pre>	<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'Specific Data Points' frags: [ParaFrag(tag='b', bold=1, fontName='Helvetica-Bold', fontSize=8, greek=0, italic=0, link=[], rise=0, text='Specific Data Points', textColor=Color(.266667,.266667,.266667,1), us_lines=[])] style: 'bulletText': None 'debug': 0) #Paragraph</pre>
Device and technical data	IP address, browser type and version, device type, operating system, screen resolution
Usage data	Pages visited, features used, time spent, click patterns, search queries
Location data	Approximate location derived from IP address — not precise GPS location unless you consent
Cookies and tracking	Session cookies, analytics cookies, preference cookies — see our Cookie Policy
Log data	Server logs including access times, error logs, and API calls

3. HOW WE USE YOUR PERSONAL DATA

Paragraph('caseSensitive': 1 'encoding': 'utf8' 'text': Purpose of Processing 'frags': [ParaFrag(__ tag __='b', bold=1, 'fontName='Helvetica-Bold', 'fontSize'=8, 'greek'=0, 'italic'=0, 'link'=[], 'rise'=0, 'text'='Purpose of Processing', 'textColor'=Color(.266667, .266667, .266667, 1), 'us_lines'=[[]] 'style': 'bulletText': None 'debug': 0)] #Paragraph	Paragraph('caseSensitive': 1 'encoding': 'utf8' 'text': Legal Basis (DPDP Act) 'frags': [ParaFrag(__ tag __='b', bold=1, 'fontName='Helvetica-Bold', 'fontSize'=8, 'greek'=0, 'italic'=0, 'link'=[], 'rise'=0, 'text'='Legal Basis (DPDP Act)', 'textColor'=Color(.266667, .266667, .266667, 1), 'us_lines'=[[]] 'style': 'bulletText': None 'debug': 0)] #Paragraph	Paragraph('caseSensitive': 1 'encoding': 'utf8' 'text': Data Used 'frags': [ParaFrag(__ tag __='b', bold=1, 'fontName='Helvetica-Bold', 'fontSize'=8, 'greek'=0, 'italic'=0, 'link'=[], 'rise'=0, 'text'='Data Used', 'textColor'=Color(.266667, .266667, .266667, 1), 'us_lines'=[[]] 'style': 'bulletText': None 'debug': 0)] #Paragraph
Providing the Platform and our services	Contract performance / Consent	Account data, User Content
Processing payments and managing subscriptions	Contract performance	Payment data, Account data
Customer support and communication	Contract performance / Legitimate interest	Account data, Communication data
Sending product updates and newsletters	Consent (opt-in required)	Name, Email
Security monitoring and fraud prevention	Legitimate interest / Legal obligation	Device data, Usage data, Log data
Analytics and product improvement	Legitimate interest	Usage data, Device data (anonymised)
Legal compliance and regulatory obligations	Legal obligation	As required by law
Enforcing our Terms of Service	Legitimate interest	All data as relevant

4. SHARING YOUR PERSONAL DATA

4.1 We do not sell your personal data. We share personal data only in the following circumstances:

- **Service providers (Data Processors):** We share data with trusted third-party vendors who help us provide the Platform, including cloud hosting providers, payment gateways, email service providers, analytics tools, and customer support software. Each processor is bound by a Data Processing Agreement requiring equivalent data protection standards.
- **Legal obligations:** We may disclose data to comply with applicable law, court orders, regulatory requests, or to protect the rights, property, or safety of the Company, our users, or the public.
- **Business transfers:** In the event of a merger, acquisition, or sale of assets, your data may be transferred as part of that transaction. We will notify affected users of any such transfer.
- **With your consent:** We may share your data with third parties where you have given us specific consent to do so.

Key third-party processors used	[List main processors — e.g. AWS for hosting / Razorpay for payments / Google Analytics for analytics / Intercom for support]
Cross-border data transfers	[Yes — data stored on servers in [country/region] / No — all data stored in India only]
Safeguards for cross-border transfers	[Standard contractual clauses / Adequacy decision / Data localisation — specify]

5. YOUR RIGHTS UNDER THE DPDP ACT 2023

<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'Your Right' frags: [ParaFrag(tag: 'b', bold: 1, fontName: 'Helvetica-Bold', fontSize: 8, greek: 0, italic: 0, link: [], rise: 0, text: 'Your Right', textColor=Color(266667, 266667, 266667, 1), us_lines=[])] style: 'bulletText: None' debug: 0) #Paragraph</pre>	<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'What It Means' frags: [ParaFrag(tag: 'b', bold: 1, fontName: 'Helvetica-Bold', fontSize: 8, greek: 0, italic: 0, link: [], rise: 0, text: 'What It Means', textColor=Color(266667, 266667, 266667, 1), us_lines=[])] style: 'bulletText: None' debug: 0) #Paragraph</pre>	<pre>Paragraph(caseSensitive: 1 encoding: 'utf8' text: 'How to Exercise' frags: [ParaFrag(tag: 'b', bold: 1, fontName: 'Helvetica-Bold', fontSize: 8, greek: 0, italic: 0, link: [], rise: 0, text: 'How to Exercise', textColor=Color(266667, 266667, 266667, 1), us_lines=[])] style: 'bulletText: None' debug: 0) #Paragraph</pre>
Right to access	Know what personal data we hold about you and how it is used	Email privacy@yourcompany.com
Right to correction	Have inaccurate or incomplete data corrected	Email or account settings
Right to erasure	Request deletion of your personal data (subject to legal retention obligations)	Email privacy@yourcompany.com
Right to grievance redressal	Raise a grievance with our Grievance Officer and escalate to the Data Protection Board	Contact Grievance Officer (details above)
Right to nominate	Nominate a person to exercise your rights in the event of death or incapacity	Email with nomination details
Withdraw consent	Withdraw consent where processing is consent-based (may affect service availability)	Account settings or email

6. DATA RETENTION

Account data	For the duration of your account plus [3] years after account deletion, or as required by law
Transaction and payment records	[7] years — as required by applicable tax and accounting law
Communication data (support tickets)	[2] years from last interaction
Usage and analytics data	[2] years — in anonymised / aggregated form only after [6] months
Legal hold data	As long as required for any pending legal proceedings or regulatory obligations

6.1 When retention periods expire, we securely delete or anonymise personal data. We may retain anonymised, aggregated data that cannot identify any individual for as long as needed for analytics and product improvement.

7. DATA SECURITY

7.1 We implement appropriate technical and organisational security measures to protect your personal data against unauthorised access, alteration, disclosure, or destruction. Our security measures include: encryption of data in transit (TLS/HTTPS) and at rest; access controls and role-based permissions; regular security audits and penetration testing; employee security training; and incident response procedures. Despite our efforts, no system is 100% secure. Please notify us immediately at [security@yourcompany.com] if you suspect any breach.

8. CHILDREN'S PRIVACY

8.1 Our Platform is not directed at children below the age of 18. We do not knowingly collect personal data from children. Under the DPDP Act 2023, processing of children's data requires verifiable parental consent. If you believe we have inadvertently collected a child's data, please contact us immediately at [privacy@yourcompany.com] and we will delete it promptly.

9. UPDATES TO THIS POLICY

9.1 We may update this Privacy Policy from time to time. When we make material changes, we will notify registered users by email and by displaying a prominent notice on the Platform before the changes take effect. The updated Policy will indicate the date of last revision. Continued use of the Platform after the effective date of the revised Policy constitutes acceptance.

10. CONTACT AND GRIEVANCE MECHANISM

Grievance Officer Name	[Name of designated Grievance Officer]
Grievance Officer Designation	[Designation]
Grievance Officer Email	[grievance@yourcompany.com]
Grievance Officer Phone	[Phone number]
Response Timeline	We will acknowledge your grievance within [48 hours] and resolve it within [30] days
Escalation to Data Protection Board	If your grievance is not resolved satisfactorily, you may contact the Data Protection Board of India at [www.dpb.gov.in]

IMPORTANT NOTE

The DPDP Act 2023 and its implementing rules impose significant obligations on Data Fiduciaries including consent notice requirements, data minimisation, purpose limitation, accuracy obligations, storage limitation, and security safeguards. Significant Data Fiduciaries (processing large volumes of sensitive personal data) face additional obligations. Consult a privacy law specialist before publishing. Template only — not legal advice.