PRIVACY POLICY

Sapience Studios

Digital Transformation · Artificial Intelligence · Enterprise Software · Creative Technology · Cloud & Automation

Document Version: 1.0 · Effective Date: 1 April 2026 · Last Updated: 26 July 2026

This Privacy Policy describes how Sapience Studios collects, uses, discloses, transfers, stores, and protects personal data. It is provided in accordance with the Digital Personal Data Protection Act, 2023 (India) ("DPDP Act"), the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, together with internationally recognised privacy principles. It is structured so it can be adapted to the EU General Data Protection Regulation (GDPR), UK GDPR, the California Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA), and other international privacy frameworks as our business expands.

1. Overview and Scope

Sapience Studios ("we", "us", "our", or the "Company") is a technology consulting practice that provides digital transformation, artificial intelligence, enterprise software, creative technology, business intelligence, cloud infrastructure, automation, and digital experience services to businesses, government entities, and individuals.

This Privacy Policy applies to:

1. **This website** (https://sapiencestudios.com and any related sub-domains or sub-brands, including Lucid Labs) and any present or future websites, applications, or digital properties we operate (together, the "Website");
2. **Prospective and existing clients and business partners**, and the personnel, representatives, and end-users of such organisations; and
3. **Job applicants, internship candidates, and individuals who contact us** through any channel, including the Website, email, social media, or otherwise.

Where we provide services to a client (a "Client"), the terms of the applicable written agreement between us and that Client govern the processing of any Client-related data. This Privacy Policy does not, and is not intended to, govern the processing of a Client's own personal data by the Client as a data fiduciary, nor the personal data of a Client's employees, customers, or end-users, except as described in Section 17 (Client Engagements).

This policy describes our privacy practices as they exist today. Our services, the channels through which we operate, and the technology we use evolve. We may update this policy from time to time in accordance with Section 22 (Updates to This Policy).

2. Who We Are and How to Contact Us

Grievance Officer: Dr. Aditya Reddy — responsible for addressing questions, complaints, and requests relating to personal data under this policy.

Contact:

- Email: privacy@sapiencestudios.com
- Registered Office: Sapience Studios, Phase-I, Electronic City, Bengaluru, Karnataka 560099, India
- Website: https://sapiencestudios.com

Any communication under this policy should identify the individual making the request and the nature of the request. We may require reasonable verification of identity before acting on a request, as permitted by applicable law.

---

3. Our Roles: Data Fiduciary and Data Processor

We act in two distinct capacities, and the rights and obligations that apply to us differ accordingly:

1. **As a Data Fiduciary** (a "controller" in some jurisdictions), we determine the purposes and means of processing personal data we collect directly, including information submitted through this Website, information provided to us in the course of a prospective or existing business relationship, and information provided by applicants to roles at Sapience Studios.
2. **As a Data Processor** (or, in some engagements, as a data fiduciary for the processing within our own business), we may process personal data on behalf of and at the direction of a Client while delivering services. In such cases, the Client remains responsible for the lawfulness of the processing, and our processing is governed by the applicable written agreement and by this policy to the extent it applies.

This distinction is important. If you provide personal data to one of our Clients rather than to us, our Client's privacy policy and instructions govern that data, not this policy. We process such data only to the extent necessary to deliver the services agreed with the Client and in accordance with the Client's lawful instructions.

---

4. Information We Collect

We collect only information that is reasonably necessary for the purposes described in this policy. We do not engage in indiscriminate or speculative collection of personal data.

4.1 Information You Provide to Us

Discovery and enquiry information. When you contact us through our Website, we collect the information you choose to submit through our discovery form, which includes: your name, the name of your organisation, your email address, your role (optional), your mobile number, and the nature of your business model and requirements. This information is used to assess whether an engagement is a fit for our practice and to respond to your enquiry.

Recruitment information. When you apply for a role or an internship, or otherwise express interest in working with us, we may collect: your name, email address, phone number, resume or curriculum vitae (including the file you upload), your LinkedIn profile URL (where provided), and any additional information you include in your application or correspondence.

Business relationship information. When you engage with us as a client, vendor, partner, or other business contact, we may collect business contact details such as your name, job title, organisation, business email address, business phone number, and information necessary to establish, perform, and administer the engagement.

Correspondence. When you contact us by email or otherwise, we may retain the contents of the correspondence and the information you provide in it.

4.2 Information Collected Automatically

Like most websites, we receive certain information automatically when you visit the Website. This is limited to standard technical data transmitted by your device and the networks you use, which may include:

- IP address and general geographic location derived from it;
- device type, operating system, browser type and settings;
- pages visited, referring pages, and the date and time of access; and
- performance and error information.

This information is collected primarily at the infrastructure and hosting layer by our hosting provider (see Section 9) in connection with the secure operation, monitoring, and improvement of the Website. It does not include advertising trackers, and we do not use it to profile you for advertising purposes.

4.3 Information We Do Not Collect

We do not currently operate advertising trackers, third-party advertising cookies, or third-party analytics pixels, and we do not sell personal data. This Website does not use cookies; it stores a single user preference (your chosen display theme) in your browser's local storage, which is not transmitted to us or to any third party. If we introduce cookies, analytics, or similar technologies in the future, we will update this policy and, where required by law, obtain your consent in advance.

4.4 Sensitive Personal Data

We generally do not seek to collect sensitive personal data (as defined under applicable Indian law, including data relating to passwords, financial information such as bank or card details, physical, physiological or mental health condition, sexual orientation, medical records or history, or biometric information). We will not collect sensitive personal data unless:

1. the collection is required in connection with a lawful engagement and you have consented to its processing; or
2. you voluntarily provide it to us (for example, in a resume or correspondence).

To the extent we process sensitive personal data, we will do so in accordance with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and the DPDP Act, and we will limit its collection and use to what is necessary for the stated purpose.

5. How We Use Information

We use personal data only for purposes that are lawful, specific, and reasonably necessary. These purposes include:

1. **Responding to you.** To respond to enquiries submitted through the Website, assess whether an engagement is a fit for our practice, and manage communication with prospective and existing clients and partners.
2. **Providing services.** To perform, administer, and deliver services under a written engagement, including communicating with Client personnel, and to comply with the Client's lawful instructions in connection with such services.
3. **Recruitment.** To evaluate applications, assess suitability for roles and internships, and maintain records relating to the recruitment process.
4. **Business operations.** To operate, secure, and improve the Website and our internal systems; to keep internal records; to manage vendors, partners, and business relationships; and to administer our business generally.
5. **Legal compliance.** To comply with legal, regulatory, and audit obligations, to prevent and investigate fraud and misuse, to establish or defend legal claims, and to enforce our agreements.
6. **Aggregate measurement.** To measure aggregate traffic and performance of the Website at the infrastructure layer in order to keep it fast and reliable. This measurement is anonymous, sets no advertising cookies, and is not used to identify you individually.

We do not use personal data collected through the Website for purposes that are incompatible with the purposes described in this policy without providing you with appropriate notice and obtaining consent where required by law.

---

6. Lawful Bases for Processing

We process personal data on one or more of the following bases:

Purpose	Lawful basis (India)	Corresponding basis (for GDPR/UK GDPR adaptation)
Responding to enquiries and assessing engagements	Consent (DPDP Act); legitimate interests of the Company	Consent; legitimate interests; contract negotiations
Providing services under an engagement	Contract; legitimate interests	Contract; legitimate interests
Recruitment and internships	Consent; legitimate interests; obligations relating to employment	Legitimate interests; consent where required
Business operations and security	Legitimate interests; legal obligations	Legitimate interests; legal obligations
Legal compliance and defence of claims	Legal obligations; legitimate interests	Legal obligations; legitimate interests

Where we rely on consent, you may withdraw it at any time (see Section 15). Where we rely on legitimate interests, we weigh our interests (or those of a third party) against your interests, fundamental rights, and freedoms. If you object to processing on legitimate-interest grounds, you may raise the matter with us as described in Section 14.

---

7. Cookies, Local Storage, and Tracking

This Website does not currently set cookies and does not use third-party advertising or analytics cookies. The only client-side storage used is a display theme preference stored in your browser's local storage (under the key `sapience-theme`). This preference remains on your device, is not transmitted to us, and can be cleared through your browser settings.

If we introduce cookies, analytics services, or similar technologies in the future, this policy will be updated to describe them, and where consent is required by applicable law, we will obtain it before deployment.

---

8. How We Share Information

We do not sell, rent, or trade personal data, and we do not share personal data for the marketing purposes of third parties. We disclose personal data only in the limited circumstances described below, and only to the extent necessary:

1. **Service providers.** We may share personal data with service providers who help us operate our business, host the Website, deliver communications, and provide professional services, subject to contractual obligations of confidentiality and data protection consistent with this policy. See Section 9.
2. **Clients and engagement parties.** In connection with delivering services to a Client, we may disclose information to the Client, its affiliates, and its authorised representatives, as directed by the Client and as necessary to perform the engagement.
3. **Professional advisers.** We may disclose personal data to our legal, accounting, tax, insurance, and other professional advisers where reasonably necessary.

4. **Legal and regulatory authorities.** We may disclose personal data where we are required to do so by law, regulation, court order, governmental or statutory authority (including law enforcement and regulatory bodies), or where disclosure is otherwise necessary to establish, exercise, or defend legal claims, to protect our rights, property, or safety or the rights, property, or safety of others, or to comply with the DPDP Act or other applicable law.
5. **Business transitions.** If we are involved in a merger, acquisition, reorganisation, sale of assets, financing, or similar transaction, personal data may be disclosed or transferred as part of that transaction, subject to appropriate confidentiality obligations.

We require recipients to process personal data consistently with this policy and applicable law. Where the SPDI Rules or the DPDP Act require a written consent or contract for a particular disclosure, we obtain it before disclosure.

---

9. Data Processors and Service Providers

We use a limited number of service providers, which may change over time. As of the effective date of this policy, the categories of service providers we use include:

Category	Provider	Role / Data involved
Hosting, CDN, and edge infrastructure	Cloudflare, Inc.	Website hosting, DNS services, edge network, and security services; standard edge and request logs (IP addresses and request metadata)
Web-font delivery	Fontshare (ITF, Fontshare.com)	Serving font files to your browser; receives limited request metadata (including IP address)
Professional advisers	Legal, accounting, and insurance advisers	Advising on compliance and protecting our legal interests

Email aliases used by Sapience Studios (including privacy@sapiencestudios.com) are managed under the Sapience Studios domain and are not separate third-party processors. Additional email delivery providers (such as Resend, Amazon SES, Microsoft 365, or Google Workspace) will be listed here only once they are actually implemented.

When we engage service providers who process personal data on our behalf, we enter into written arrangements requiring them to process personal data only for our documented instructions, to implement reasonable security safeguards, and to cooperate with us in fulfilling data-principal requests.

---

10. International Data Transfers

The Website is served globally through cloud infrastructure operated by our hosting provider. As a result, personal data may be processed in jurisdictions other than the one in which you reside, including India and other countries where we or our service providers operate.

We will ensure that any cross-border transfer of personal data complies with applicable law. In particular, we will not transfer personal data to a country or territory that the Government of India has restricted under Section 16 of the DPDP Act, unless permitted under the applicable rules. For transfers to other

jurisdictions, including for visitors subject to the GDPR, UK GDPR, or CCPA/CPRA, we will rely on appropriate or suitable safeguards, including (where applicable) the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, or equivalent recognised transfer mechanisms.

---

11. **Data Retention**

We will only keep personal data for as long as reasonably necessary to fulfil the purposes we collected it for. We may keep your personal data for a longer period to comply with our legal obligations or in the event of a complaint or litigation. We have established retention guidelines by category:

Category	Indicative retention
Website enquiry and discovery submissions	Retained as long as needed to evaluate and respond to the enquiry, and thereafter for a reasonable period for our records and to defend potential claims
Recruitment and internship applications	Retained for the duration of the relevant hiring process and for a reasonable period thereafter for our records; longer where you have agreed to be considered for future opportunities
Business relationship and engagement records	Retained for the duration of the relationship and for such further period as required by the applicable agreement, law, or limitation periods
Client engagement data	Retained in accordance with the applicable written agreement and applicable law
Infrastructure and request logs	Retained in accordance with our hosting provider's standard retention practices

Where retention is no longer necessary, we delete or irreversibly anonymise the personal data in accordance with our internal procedures. Nothing in this section prevents us from retaining personal data where required by law or where necessary to establish, exercise, or defend legal claims.

---

12. **Security Safeguards**

We implement reasonable security safeguards to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks, in accordance with the DPDP Act, the SPDI Rules, and accepted industry practice. Our safeguards include:

- encryption of data in transit using industry-standard transport-layer security (TLS);
- access controls and least-privilege principles, limiting access to personal data to personnel who need it to perform their duties;
- confidentiality obligations on our personnel and service providers;
- secure development practices and routine maintenance of our systems and the Website;
- monitoring and logging at the infrastructure layer to detect and respond to anomalies; and
- procedures for the secure disposal or anonymisation of personal data when it is no longer needed.

While we take reasonable and appropriate measures to protect personal data, no method of transmission or storage is completely secure. We cannot guarantee the absolute security of any information you transmit to us, and you provide information at your own risk. Where we engage service providers, we require them to maintain safeguards consistent with this policy and applicable law.

---

13. Children's Data

Our services are directed to businesses and professionals and are not designed for children. We do not knowingly collect personal data from children, and under the DPDP Act a "child" is an individual below the age of eighteen (18) years. If we learn that we have collected personal data from a child without verifiable parental consent, we will take reasonable steps to delete such data promptly. If you believe we have collected data relating to a child, please contact us using the details in Section 2.

---

14. Your Rights

Subject to applicable law and to reasonable verification of your identity, you may have the following rights in respect of personal data we hold about you as a data fiduciary:

1. **Right to access.** To obtain confirmation of whether we process personal data about you and a summary of the personal data processed, the purposes of processing, and the recipients of that data.
2. **Right to correction.** To require us to correct or update incomplete or inaccurate personal data.
3. **Right to erasure.** To request the erasure of personal data, subject to applicable legal and contractual retention requirements.
4. **Right to withdraw consent.** To withdraw any consent you have given to the processing of your personal data, which will not affect the lawfulness of processing carried out before withdrawal.
5. **Right to grievance redressal.** To lodge a grievance with us regarding the processing of your personal data, and to escalate any unresolved grievance to the Data Protection Board of India or other competent authority as provided by applicable law.

Where we process personal data as a processor on behalf of a Client, requests relating to such data should be directed to the relevant Client. We will cooperate with the Client in responding to such requests to the extent required by applicable law and the applicable agreement.

Where a data-protection law that applies to you (for example, the GDPR, UK GDPR, or CCPA/CPRA, where we are subject to it) grants you additional rights — including rights to data portability, restriction of processing, and objection to processing — those rights shall apply to the extent required by the law applicable to you.

To exercise any of these rights, contact us at the details in Section 2. We will respond within the timeframes prescribed by applicable law, which is generally thirty (30) days under the SPDI Rules and forty-five (45) days under the DPDP Act. If we require more time, we will inform you and explain the reason.

15. Consent Withdrawal

Where we process personal data on the basis of your consent, you may withdraw that consent at any time by contacting us at the details in Section 2. Withdrawal will not affect the lawfulness of processing based on consent before its withdrawal, and may prevent us from providing certain services or responding to your enquiry. Where processing continues on a basis other than consent (for example, performance of a contract or compliance with law), withdrawal of consent does not require us to cease such processing.

16. Grievance Redressal

If you have a complaint about our privacy practices, please contact our Grievance Officer, Dr. Aditya Reddy, at the details in Section 2. We will acknowledge your complaint and respond within the timeframes required by applicable law. If you are not satisfied with our response, you may escalate the matter to the Data Protection Board of India or such other authority as may be prescribed under the DPDP Act, and, where applicable, to your local data-protection supervisory authority.

17. Client Engagements

When we provide services to a Client, we may receive or access personal data belonging to the Client's employees, customers, or end-users ("Client Data"). Our treatment of Client Data is governed by the following principles:

1. We process Client Data only for the purposes and in the manner instructed by the Client and as necessary to deliver the services, in accordance with the applicable written agreement.
2. The Client is responsible for ensuring that its collection and disclosure of Client Data to us is lawful, including obtaining any required consents and providing any required notices.
3. Unless otherwise agreed, Client Data is not used to train our general-purpose models, to improve services for other clients, or for purposes unrelated to the engagement.
4. We implement safeguards and access controls to limit access to Client Data to personnel engaged on the applicable engagement.
5. On completion or termination of an engagement, we will return or securely destroy Client Data as instructed by the Client and in accordance with the applicable agreement, unless we are required by law to retain it.
6. Our case studies and portfolio are anonymised by design: projects are described by type, industry vertical, and geographic region, and client identities and confidential information are withheld.

Nothing in this policy is intended to create obligations with respect to Client Data beyond those set out in the applicable written agreement and applicable law.

18. Marketing Communications

We may, where permitted by law and with your consent where required, send you communications about our practice, services, and insights. You may opt out of such communications at any time by following the

unsubscribe instructions in any such communication or by contacting us at the details in Section 2. We do not currently operate an advertising or marketing network, and we will not use personal data collected through the Website for third-party marketing purposes.

---

19. Third-Party Links and Services

The Website may contain links to third-party websites, social media platforms, and services (such as LinkedIn and Twitter/X). We do not control, and are not responsible for, the privacy practices or content of those third parties. Your use of any linked service and any information you provide to it is governed by that third party's own terms and privacy policy. We encourage you to review the privacy practices of any third party before providing information to it.

---

20. Data Breach Notification

In the event of a data breach involving personal data, we will take reasonable steps to contain the breach, assess the risk posed to affected data principals, and, where required by the DPDP Act or other applicable law, notify the Data Protection Board of India and affected data principals without undue delay. We maintain internal procedures for the detection, escalation, and management of security incidents.

---

21. Business Transfers

If we undergo a merger, acquisition, reorganisation, divestiture, or sale of all or a substantial portion of our assets, personal data held by us may be transferred to the acquiring or successor entity. We will take reasonable steps to ensure that the recipient maintains standards of data protection consistent with this policy and applicable law, and we will update this policy as required.

---

22. Updates to This Policy

We may update this policy from time to time to reflect changes in our practices, services, technology, or legal requirements. Material changes will be reflected by an updated version number and effective date at the top of this policy and will be published on the Website. Where required by applicable law, we will obtain your consent to any material change that affects your rights. Your continued use of the Website or services after the effective date of a revised policy constitutes acceptance of the revised policy to the extent permitted by law.

---

23. Governing Law and Jurisdiction

This Privacy Policy shall be governed by and construed in accordance with the laws of India. Subject to applicable law, the courts located in Bengaluru, Karnataka, shall have exclusive jurisdiction over any disputes arising out of or relating to this Privacy Policy.

24. Definitions

- **Data Principal:** an individual to whom personal data relates. Where the individual is a child, a data principal includes their parents or lawful guardian.
- **Personal Data:** any data about an individual who is identifiable by or in relation to such data, as defined under the DPDP Act.
- **Data Fiduciary:** any person who, alone or jointly with others, determines the purpose and means of processing personal data (referred to as a "controller" in some jurisdictions).
- **Data Processor:** any person who processes personal data on behalf of a Data Fiduciary.
- **Data Breach:** a breach of security safeguards leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored, or otherwise processed.
- **Sensitive Personal Data / Sensitive Personal Data or Information (SPDI):** as defined under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, including passwords, financial information, health or medical records, sexual orientation, biometric information, and such other information as may be notified.

25. Version History

Version	Effective date	Last updated	Summary of changes
1.0	1 April 2026	26 July 2026	Initial publication.

© 2026 Sapience Studios. All rights reserved.