Proprietary Information. Not to be reproduced or made available to third parties without consent from Secure Minds Private Limited. © 2026

Privacy Policy
Version 1.0

Issued under the Digital Personal Data Protection Act, 2023
and the Digital Personal Data Protection Rules, 2025
Effective: 11 August 2026

Document Revision History

Date	Version	Description of change and reason	Author	Reviewer	Approver
August 11, 2026	1.0	Initial Approved Version	Jatin	Sachin Chadha	Bharti Chadha

Table of Contents

1. Introduction 4
1.1 Purpose 4
1.2 Scope 4
1.3 Objective 4
1.4 Privacy Principles 4
2. Policy Statement 5
2.1 Who We Are and Our Role 5
2.2 Personal Data We Collect and Why 5
2.3 Consent and Withdrawal 6
2.4 Cookies and Similar Technologies 6
2.5 Sharing of Personal Data 7
2.6 Transfers Outside India 7
2.7 Data Retention 7
2.8 Security Safeguards and Breach Notification 8
2.9 Rights of Data Principals 8
2.10 Children 9
2.11 Additional Information for the EU and UK 9
3. Grievance Redressal and Contact 9
4. Policy Review and Maintenance 10

1. Introduction

1.1 Purpose

This policy explains how Secure Minds Private Limited ("Secure Minds", "we", "us") collects, uses, shares, retains and protects personal data, and how individuals can exercise their rights. It is issued under the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"). As a cybersecurity and GRC consultancy, we hold ourselves to the same standard of privacy and security we advise our clients on.

1.2 Scope

This policy applies to personal data we process when an individual:

(a) visits secureminds.pro or interacts with our pages, forms or links;

(b) contacts us by email, phone, WhatsApp, LinkedIn or a website form;

(c) is, or works for, a client, prospective client, partner, vendor or subcontractor of Secure Minds;

(d) receives business communications from us, including outreach about our services; or

(e) attends a webinar, training session or event we run.

Not covered by this policy: job applicants and candidates, who are covered by our Candidate Privacy Notice; our employees and contractors, who are covered by an internal notice given at onboarding; and personal data we process on behalf of clients during an engagement (see section 2.1).

1.3 Objective

- Process personal data lawfully, fairly and transparently, for clear and specified purposes.
- Collect only the personal data necessary for those purposes.
- Give individuals a clear way to consent, withdraw consent and exercise their rights.
- Protect personal data with reasonable security safeguards and respond to breaches promptly.
- Comply with the DPDP Act, the DPDP Rules and other applicable privacy laws and contractual obligations.

1.4 Privacy Principles

- **Lawfulness and consent:** personal data is processed only on a lawful ground, with free, specific, informed and unambiguous consent where consent is the ground.
- **Purpose limitation:** personal data is used only for the purpose stated at collection.
- **Data minimisation:** we collect only what the purpose needs.
- **Accuracy:** we keep personal data accurate, complete and up to date.
- **Storage limitation:** we erase personal data once the purpose is served, unless the law requires us to keep it.
- **Security:** we apply reasonable security safeguards to prevent personal data breaches.

- **Accountability:** Secure Minds is responsible for compliance, including processing carried out by our Data Processors.

2. Policy Statement

2.1 Who We Are and Our Role

Secure Minds Private Limited, CIN U72900DL2020PTC367845, provides GRC advisory, security assessment, virtual CISO/DPO, and talent and staffing services to organisations in India and internationally.

- **Registered office:** A-163, G No. 16, Pratap Nagar, Mayur Vihar Phase-1, East Delhi, Delhi 110091, India
- **Operating address:** 02-007, 2nd Floor, Emaar The Palm Square, Sector-66, Gurugram, Haryana 122102, India
- **Website:** www.secureminds.pro

Situation	Our role	Who decides how the data is used
Website visits, enquiries, marketing, client and vendor relationship management	**Data Fiduciary**	Secure Minds, under this policy
Delivering a client engagement (e.g. ISO/IEC 27001 or SOC 2 audit and readiness, VAPT, phishing simulation, vCISO/vDPO services) where we access the client's personal data	**Data Processor**	Our client, under its own privacy notice and our contract with it

Where we act as a Data Processor, we process personal data only on our client's documented instructions and for the engagement's purpose. We keep it confidential and secure, and we return or erase it when the engagement ends, unless the law requires us to keep it. Individuals whose data was shared with us by a client should contact that client first; we will assist the client in responding.

2.2 Personal Data We Collect and Why

Who you are	Personal data	Purpose	Basis under the DPDP Act
Enquirer (email, phone, WhatsApp, LinkedIn)	Name, business email, phone, organisation, country, the content of your message	To respond, scope our services and send a proposal	Data voluntarily provided for that purpose (s.7(a))
Partner applicant (Partner With Us form)	Organisation, contact person, email, phone, partnership type, area of focus, years in operation, notes	To assess and set up a partnership	Consent (s.6), given on the form
Client or prospective client contact	Name, designation, business email and phone, meeting notes, contract and billing details	To negotiate and perform our contract, invoice and manage the relationship	Data provided for the purpose (s.7(a)); legal obligations such as GST and tax records (s.7(c))
Business outreach recipient	Name, designation, employer, business email or phone, public professional profile (e.g. LinkedIn)	To tell you about our services where relevant to your role	Data you made public (s.3(c)(ii)); otherwise consent (s.6). You can opt out at any time

Who you are	Personal data	Purpose	Basis under the DPDP Act
Vendor, subcontractor or recruitment partner contact	Name, business contact details, bank and tax details needed for payment	To engage and pay you	Data provided for the purpose (s.7(a)); legal obligations including TDS (s.7(c))
Event or training attendee	Name, email, organisation, attendance and feedback	To register you, deliver the session and issue certificates	Consent (s.6)
Website visitor	IP address, browser and device data, pages viewed, referrer, timestamps; security and login logs	To operate and secure the website and detect misuse	Necessary to provide the service requested; legal obligations under CERT-In Directions (s.7(c))
Website visitor who accepts analytics	Clicks, scrolls, heatmaps and session recordings (form inputs masked)	To understand how pages are used and improve them	**Consent only (s.6)**, via our cookie banner. Off by default

- **What we do not want:** please do not send us government identifiers (Aadhaar, PAN, passport), financial account numbers, health information, or any personal data of children through our website or enquiry channels.
- **What we do not do:** we do not sell or rent personal data, use it for profiling or behavioural advertising, track individuals across other websites, or make decisions about individuals solely by automated means.

2.3 Consent and Withdrawal

Where we rely on consent, we ask for it through a clear affirmative action, such as ticking a box or choosing "Accept" on our cookie banner. Each request is backed by a notice stating the personal data and the purpose, and consent is limited to that purpose. Withdrawing consent is as easy as giving it (s.6(4)):

- **Analytics cookies:** use Cookie Settings in the website footer, at any time.
- **Outreach and marketing:** reply "Unsubscribe" or "STOP", use the opt-out link, or write to privacy@secureminds.pro.
- **Anything else:** write to privacy@secureminds.pro.

Withdrawal does not affect processing done before it. On withdrawal we stop the processing within a reasonable time and erase the data, unless another lawful ground requires us to keep it, and we instruct our Data Processors to do the same (s.6(6)).

2.4 Cookies and Similar Technologies

Strictly necessary cookies are always on. Analytics cookies are set only after you choose "Accept", and you can change your choice at any time in Cookie Settings.

Category	Provider	Examples	Lifetime	Default
Strictly necessary	Secure Minds (WordPress, security plugins)	Consent record, session and security cookies, wordpress_test_cookie	Session to 12 months	On

Category	Provider	Examples	Lifetime	Default
Analytics: session replay and heatmaps	Hotjar Ltd.	_hjSessionUser_*, _hjSession_*	30 minutes to 12 months	**Off until consent**
Analytics: session replay and heatmaps	Microsoft Corporation (Clarity)	_clck, _clsk, CLID, MUID	1 day to 12 months	**Off until consent**
Analytics: traffic measurement	Google LLC (Google Analytics 4, via Site Kit)	_ga, _ga_*	Up to 2 years	**Off until consent**

Cookie names and lifetimes are set by each provider and may change. We review this table whenever we add, change or retire a website tool. Cookie Settings in the website footer always shows the cookies currently in use, and you can delete cookies at any time through your browser settings.

2.5 Sharing of Personal Data

We share personal data only as needed for the purposes in section 2.2:

- **Service providers (Data Processors)** acting on our instructions under written contracts: website hosting, email and collaboration, cloud storage, analytics (only with consent), CRM and lead-management tools, and our accountants and auditors.
- **Subcontractors and associate consultants** engaged on a client project, under confidentiality and data-protection terms equivalent to ours.
- **Professional advisers, regulators, courts and law-enforcement agencies**, where the law requires it or to establish, exercise or defend legal claims.
- **Messaging platforms you choose to use:** if you click our WhatsApp or LinkedIn buttons, you leave our website and that platform's own privacy policy applies to what you share there.
- **A successor entity** in a merger, acquisition or restructuring, subject to this policy.

On request, we will provide the identities of the Data Fiduciaries and Data Processors we have shared your personal data with (s.11(1)(b)).

2.6 Transfers Outside India

We serve clients in North America, Europe, the Middle East and Asia-Pacific, and some of our service providers store data outside India. We transfer personal data outside India only as s.16 of the DPDP Act permits: never to a country or territory the Central Government has restricted by notification, and subject to any conditions the DPDP Rules impose. For EU and UK personal data, see section 2.11.

2.7 Data Retention

Data	Retention
Enquiries that do not become a client relationship	24 months from our last interaction, then erased
Outreach and prospect records	24 months from our last interaction, or sooner on opt-out. A minimal suppression record (name and email) is kept so we do not contact you again
Partner applications not taken forward	12 months from submission

Data	Retention
Client and vendor contract, billing and tax records	8 years from the end of the relevant financial year (Companies Act, 2013 s.128(5); CGST Act, 2017 s.36)
Client engagement data processed as a Data Processor	Per the client contract; by default returned or erased within 30 days of engagement close-out
Website security and access logs	Minimum 1 year (DPDP Rules, Rule 8(3)); 180 days within India for logs within CERT-In Directions scope
Analytics data (with consent)	Per the provider's retention setting, configured to no more than 14 months

When the purpose is fulfilled or consent is withdrawn, we erase the personal data and have our Data Processors erase it, unless the law requires retention (s.8(7)). Copies in routine backups are overwritten in the normal backup cycle, within 90 days.

2.8 Security Safeguards and Breach Notification

We apply reasonable security safeguards under s.8(5) of the DPDP Act and Rule 6 of the DPDP Rules, including:

- **Access control:** role-based, least-privilege access with multi-factor authentication on email, storage and website administration.
- **Encryption:** in transit (TLS) and at rest on our storage and collaboration platforms.
- **Monitoring:** logging and monitoring of access, with log retention to detect and investigate unauthorised access.
- **Contracts:** written confidentiality and data-protection obligations on staff, consultants and Data Processors.
- **Continuity:** backups and continuity measures to restore data if it is compromised.

Personal data breach. If a breach affects your personal data, we will inform you without delay, in plain language, of what happened, its likely consequences, what we are doing and what you can do (Rule 7(1)). We will inform the Data Protection Board of India without delay and submit a detailed report within 72 hours of becoming aware (Rule 7(2)), and report to CERT-In where its Directions require.

2.9 Rights of Data Principals

Right	What it means	DPDP Act
Access	A summary of the personal data we process, our processing activities, and the identities of those we have shared it with	s.11
Correction, completion, updating	Fix inaccurate, incomplete or outdated personal data	s.12(2)
Erasure	Delete personal data no longer needed for the purpose, unless the law requires retention	s.12(3)
Withdraw consent	At any time, as easily as it was given	s.6(4)
Grievance redressal	Have a complaint resolved by us	s.13

Right	What it means	DPDP Act
Nominate	Name a person to exercise your rights on your death or incapacity	s.14

How to exercise a right. Email privacy@secureminds.pro with the request in the subject line, from the email address we hold for you where possible. We may verify your identity before acting. We acknowledge requests within 7 days and resolve them within 30 days, and in every case within the period prescribed by the DPDP Rules, not exceeding 90 days (Rule 14(3)).

Duties of Data Principals (s.15). Comply with applicable law; do not impersonate another person; do not suppress material information when providing data for proof of identity or address; do not file a false or frivolous grievance; and provide only verifiably authentic information when seeking correction or erasure.

2.10 Children

Our website and services are intended for businesses and professionals aged 18 or over. We do not knowingly process the personal data of children (under 18) and do not track or target them (s.9). If you believe we hold a child's personal data without verifiable parental consent, write to privacy@secureminds.pro and we will erase it.

2.11 Additional Information for the EU and UK

Where the EU GDPR or UK GDPR applies to our processing (Art. 3(2)), the following also applies:

- **Controller:** Secure Minds Private Limited (details in section 2.1).
- **Legal bases (Art. 6(1)):** contract (b) for client and vendor relationships; legal obligation (c) for tax and accounting records; legitimate interests (f) for responding to enquiries, B2B outreach relevant to your role and website security; consent (a) for analytics cookies (also ePrivacy Directive Art. 5(3) / PECR reg. 6).
- **Source of data (Art. 14):** where not collected from you, from public professional profiles (e.g. LinkedIn), your organisation's website, or business-data providers.
- **Your rights:** access, rectification, erasure, restriction, portability and objection, including an absolute right to object to direct marketing (Arts. 15–21), and the right to complain to your supervisory authority (Art. 77) or, in the UK, the ICO.
- **Transfers:** India has no EU or UK adequacy decision. We rely on the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914), or the UK IDTA / Addendum, where we receive personal data from the EU or UK.

Individuals in other jurisdictions (for example Canada, Singapore and Australia) may hold additional rights under local law. Write to privacy@secureminds.pro and we will honour them where they apply.

3. Grievance Redressal and Contact

Grievance Officer: Bharti Chadha, Director, Secure Minds Private Limited

- **Email:** privacy@secureminds.pro
- **Phone:** +91 99535 65539
- **Address:** 02-007, 2nd Floor, Emaar The Palm Square, Sector-66, Gurugram, Haryana 122102, India
- **General enquiries:** contact@secureminds.pro

If you are not satisfied with our resolution, you may complain to the Data Protection Board of India under s.13(3) of the DPDP Act, after first using our grievance process.

4. Policy Review and Maintenance

This policy will be reviewed:

- At least once every year; or
- Whenever there is a significant change in the company's processing activities, technology, or the legal and regulatory environment.

The version and effective date in the Document Revision History show the current version. If a change materially affects how we use personal data already collected under consent, we will notify affected individuals and, where required, seek fresh consent.