Data Processing Agreement

Security Brigade InfoSec Private Limited, a company incorporated in India with its registered office in Mumbai, Maharashtra ("**Security Brigade**", "**we**", "**us**", or "**Processor**"), and the customer entering into the Master Services Agreement that incorporates this DPA ("**Customer**", "**you**", or "**Controller**"), agree as follows.

1. Background and definitions

This DPA applies whenever Security Brigade Processes Personal Data on behalf of Customer in the course of providing the Services under the MSA. The Services include both Customer's use of Security Brigade's platforms — in particular the Sentinel attack-surface and exposure-management platform — and engagement-based security services such as vulnerability assessment and penetration testing (VAPT), security audits, incident response, red-team and threat-hunting engagements, and managed security services. This DPA governs the parties' respective rights and obligations with respect to such Processing and is incorporated into, and forms an integral part of, the MSA.

This DPA is governed primarily by the Indian Digital Personal Data Protection Act, 2023 ("**DPDP Act**"). Where Customer is established in the European Union or the European Economic Area, or in the United Kingdom, or where the Personal Data Processed under the MSA relates to Data Subjects in those jurisdictions, this DPA is additionally governed by Regulation (EU) 2016/679 (the "**GDPR**") and the United Kingdom General Data Protection Regulation (the "**UK GDPR**") respectively, and shall be interpreted to give effect to the obligations imposed on processors under those instruments.

1.1 Definitions

In this DPA, capitalised terms have the meanings set out below. Terms used but not defined here have the meanings given to them in the MSA or in Applicable Law.

- **Personal Data** means any information relating to an identified or identifiable natural person ("data subject") within the meaning of Article 4(1) GDPR, and "personal data" as defined in §2(t) of the DPDP Act, in each case that Security Brigade Processes on behalf of Customer under the MSA.
- **Customer Personal Data** means Personal Data Processed by Security Brigade on behalf of Customer under the MSA, including (a) Personal Data Customer makes available to Security Brigade and (b) Personal Data Security Brigade accesses, collects, or generates in the course of providing the Services.
- **Processing** has the meaning given in Article 4(2) GDPR — any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction — and includes "processing" as defined in §2(x) of the DPDP Act. "**Process**" and "**Processed**" shall be construed accordingly.
- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data within the meaning of Article 4(7) GDPR, and includes a "Data Fiduciary" within the meaning of §2(i) of the DPDP Act.

- **Processor** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller within the meaning of Article 4(8) GDPR, and includes a "Data Processor" within the meaning of §2(k) of the DPDP Act.
- **Sub-processor** means any third party engaged by Security Brigade (or by another Sub-processor) to Process Customer Personal Data on behalf of Customer in connection with the Services.
- **Data Subject** means the identified or identifiable natural person to whom Personal Data relates within the meaning of Article 4(1) GDPR, and includes a "Data Principal" within the meaning of §2(j) of the DPDP Act.
- **Personal Data Breach** has the meaning given in Article 4(12) GDPR — a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- **Standard Contractual Clauses** or **SCCs** means the standard contractual clauses for the transfer of personal data to third countries set out in the Annex to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor), as such clauses may be amended or replaced from time to time.
- **UK Addendum** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner's Office, Version B1.0, in force 21 March 2022, as such addendum may be amended or replaced from time to time.
- **MSA** means the Master Services Agreement (or equivalent commercial agreement, including any statement of work, order form, or online terms of service) entered into between Customer and Security Brigade that incorporates this DPA.
- **Services** means the services that Security Brigade provides to Customer under the MSA, including Sentinel platform services and engagement-based security services such as VAPT, audits, incident response, and managed services.
- **Applicable Law** means the data-protection and privacy laws applicable to the Processing of Customer Personal Data under this DPA, including the DPDP Act, the GDPR, and the UK GDPR, as the case may be.

2. Scope and roles

For the purposes of this DPA, Customer is the Controller of Customer Personal Data and Security Brigade is the Processor. This DPA applies to all Personal Data that Customer makes available to Security Brigade, or that Security Brigade collects, generates, or otherwise accesses, in the course of providing the Services.

This DPA covers Processing in both of the following contexts: (a) Personal Data flowing through Security Brigade's platforms, including the Sentinel attack-surface and exposure-management platform and any related Security Brigade-hosted systems used to deliver the Services; and (b) Personal Data accessed, generated, or otherwise Processed by Security Brigade in the course of delivering engagement-based services, including VAPT, audits, incident response, and managed services. The subject matter, duration, nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are described per engagement in Annex A.

3. Processor obligations

Security Brigade shall:

3.1 Documented instructions

Process Customer Personal Data only on Customer's documented instructions, including those set out in the MSA, this DPA, individual statements of work, and Customer's reasonable written instructions thereafter. If Security Brigade is required by Applicable Law to Process Personal Data otherwise than as instructed by Customer, Security Brigade shall inform Customer of that legal requirement before Processing, unless that law prohibits such notice.

3.2 Confidentiality

Ensure that personnel authorised to Process Personal Data are bound by appropriate confidentiality obligations (whether contractual or statutory) and have received documented data-protection training.

3.3 Security measures

Implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Current measures are described in Annex B and reviewed at least annually.

3.4 Sub-processor engagement

Engage Sub-processors only in accordance with Section 4 and Annex C.

3.5 Data subject rights assistance

Assist Customer, taking into account the nature of the Processing and the information available to Security Brigade, by appropriate technical and organisational measures, in fulfilling Customer's obligation to respond to Data Subject requests under GDPR Articles 12–22, DPDP §11–14, or analogous provisions.

3.6 Compliance assistance

Assist Customer in ensuring compliance with the obligations pursuant to GDPR Articles 32–36 (security, breach notification, DPIA, prior consultation), DPDP §8–9, and analogous obligations under Applicable Law, taking into account the nature of Processing and the information available to Security Brigade.

3.7 Personal Data Breach notification

Notify Customer of any Personal Data Breach without undue delay and in any event within seventy-two (72) hours of becoming aware of the Personal Data Breach, providing the information required under Section 6.

3.8 End-of-term handling

On termination or expiry of the MSA, destroy or — if Customer elects in writing within thirty (30) days of termination — return Customer-supplied Personal Data, as further set out in Section 10.

3.9 Audit cooperation

Make available to Customer all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits and inspections in accordance with Section 9.

3.10 Use of large language models

Security Brigade does not transmit Customer Personal Data to large language model providers (including but not limited to Anthropic, OpenAI, and DeepSeek) as part of providing the Services. Security Brigade's use of large language models is limited to internal content generation, summarisation, and tooling that operates on Security Brigade's own data and on de-identified inputs. This commitment applies for the duration of this DPA and is independently auditable on request.

4. Sub-processor regime

4.1 General authorisation

Customer grants Security Brigade general written authorisation to engage the Sub-processors listed in Annex C for Processing of Customer Personal Data, subject to the requirements of this Section 4.

4.2 New Sub-processors

Security Brigade shall give Customer at least thirty (30) days' prior notice before adding or replacing any Sub-processor. Notice will be given by posting the updated Annex C to Security Brigade's website and, on Customer's written request, by email to a Customer-designated contact.

4.3 Right to object

Customer may object to a new Sub-processor on reasonable data-protection grounds by giving written notice within thirty (30) days of Security Brigade's notice. The parties shall work in good faith to resolve the objection. If no resolution is reached within thirty (30) days of Customer's objection, Customer may terminate the affected portion of the Services on written notice, with a prorated refund of any pre-paid Service fees attributable to the terminated portion.

4.4 Sub-processor obligations

Security Brigade shall impose, by written contract, data-protection obligations on each Sub-processor that are no less protective than those imposed on Security Brigade under this DPA. Security Brigade remains liable to Customer for the performance of each Sub-processor's obligations.

5. International transfers

5.1 EU/EEA transfers

Where Security Brigade Processes Personal Data subject to the GDPR outside the EEA, the parties incorporate by reference the Standard Contractual Clauses adopted by European Commission Implementing Decision (EU) 2021/914, Module Two (Controller to Processor), as if executed between Customer (as data exporter) and Security Brigade (as data importer). The optional clauses (Clause 7 — docking clause, and Clause 11(a) option — independent dispute resolution) are not selected. Annex I.A is populated by Annex A of this DPA; Annex I.B by Annex C of this DPA; Annex II by Annex B of this DPA. The supervisory authority for purposes of Clause 13 is the Irish Data Protection Commission for transfers from Irish-established data exporters, and the supervisory authority of the data exporter's establishment in all other cases.

5.2 UK transfers

Where Personal Data subject to the UK GDPR is transferred outside the United Kingdom, the parties additionally incorporate by reference the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (Version B1.0, in force 21 March 2022), with Tables 1, 2, and 3 deemed completed by the corresponding provisions of this DPA, and no additional protection added under Table 4.

5.3 India outbound transfers

Where Personal Data is Processed under the DPDP Act and transferred outside India, Security Brigade complies with §16 of the DPDP Act and does not transfer Personal Data to jurisdictions notified as restricted by the Central Government from time to time. Transfers are otherwise subject to any conditions imposed under §16 as the implementing rules are notified.

5.4 Localisation

Where Customer elects data-localisation under the MSA or by written notice, Security Brigade shall configure storage and backup locations accordingly. Current available regions include Mumbai, Paris, Singapore, and Dubai (further regions on request).

6. Personal Data Breach

6.1 Notification

Security Brigade shall notify Customer of any Personal Data Breach without undue delay and in any event within seventy-two (72) hours of becoming aware of the Personal Data Breach.

6.2 Content of notification

The notification shall include, to the extent then known:

- the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- the name and contact details of Security Brigade's Data Protection Officer or other contact point where more information can be obtained;
- the likely consequences of the Personal Data Breach;
- the measures taken or proposed to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.3 Follow-up

Where it is not possible to provide the information at the same time, the information may be provided in phases without further undue delay. Security Brigade shall document Personal Data Breaches comprising the facts, effects, and remedial action taken, and shall make this documentation available to Customer and to supervisory authorities as required.

7. Data subject rights assistance

7.1 Forwarding requests

If Security Brigade receives a request from a Data Subject in respect of their Personal Data, Security Brigade shall promptly forward the request to Customer and shall not respond to the request other than to acknowledge receipt and direct the Data Subject to Customer, except where required by Applicable Law.

7.2 Assistance

Security Brigade shall provide reasonable assistance to Customer, taking into account the nature of the Processing and the information available to Security Brigade, in responding to Data Subject requests for access, rectification, erasure, restriction, portability, objection, and the right not to be subject to solely automated decision-making, under GDPR Articles 12–22, DPDP §11–14, and analogous provisions of Applicable Law.

7.3 Service-level

Security Brigade shall acknowledge Data Subject-related Customer requests within forty-eight (48) hours and respond substantively within ten (10) business days, except where Customer reasonably requires faster turnaround to meet its own statutory deadlines.

8. DPIA and consultation assistance

Security Brigade shall provide Customer with reasonable assistance, on Customer's written request, with:

- data protection impact assessments under GDPR Article 35 or analogous obligations under the DPDP Act and other Applicable Law; and
- prior consultations with supervisory authorities under GDPR Article 36 or analogous obligations,

in each case to the extent the assessment or consultation relates to Personal Data Processed by Security Brigade under the MSA, and taking into account the nature of Processing and the information available to Security Brigade. Assistance beyond the provision of information reasonably within Security Brigade's possession may be subject to commercial terms agreed between the parties.

9. Audit and inspection

9.1 Audit reports

Customer's audit rights under this DPA and Applicable Law may be satisfied by Security Brigade providing, on Customer's written request:

- Security Brigade's most recent ISO/IEC 27001 certificate and statement of applicability; and
- (when available) Security Brigade's most recent SOC 2 Type II report. Security Brigade's SOC 2 Type II attestation is in progress.

9.2 On-site inspection

Where the reports in Section 9.1 are not sufficient to demonstrate compliance with this DPA, Customer may, on at least thirty (30) days' prior written notice and not more than once per twelve-month period (additional inspection rights apply post Personal Data Breach), conduct or appoint an independent third-party auditor to conduct an inspection of Security Brigade's relevant facilities, processes, and records. The inspection shall:

- be conducted during normal business hours;
- be subject to confidentiality obligations no less protective than those in the MSA;
- not unreasonably interfere with Security Brigade's operations;
- exclude information of other customers and Security Brigade's commercially-sensitive information not required to verify compliance with this DPA; and
- be limited in scope to Security Brigade's compliance with this DPA.

Costs of the inspection are borne by Customer, except where the inspection reveals a material non-compliance, in which case Security Brigade shall reimburse Customer's reasonable inspection costs.

9.3 Post-breach inspection

The frequency limit in Section 9.2 does not apply to an inspection conducted following a Personal Data Breach, which may be conducted on shorter notice reasonable in the circumstances.

10. Term, termination, and destruction

10.1 Term

This DPA is effective on the Effective Date set out at the top of this document and remains in force for as long as Security Brigade Processes Customer Personal Data under the MSA.

10.2 Destruction by default

On termination or expiry of the MSA, Security Brigade shall destroy all Customer Personal Data in its possession or control, including any backups and archived copies, subject to Section 10.4 (statutory retention).

10.3 Customer-elected return

Customer may, by written notice given prior to or within thirty (30) days after termination or expiry of the MSA, elect to have Customer-supplied Personal Data returned in a commercially-reasonable, machine-readable format (CSV, JSON, or as otherwise agreed) before destruction. The right of return:

- applies only to Personal Data that Customer supplied to Security Brigade, and does NOT apply to Security Brigade work product (including but not limited to security findings, vulnerability reports, test evidence, audit reports, code review outputs, threat models, and analytical content generated by Security Brigade in the course of providing the Services), which remains the property of Security Brigade;
- does not extend the destruction timelines in Section 10.4.

10.4 Destruction timeline

Destruction is completed within the following windows:

- live production systems and copies: within thirty (30) days of termination or expiry;
- backup and archival systems: within ninety (90) days of termination or expiry;
- Personal Data retained pursuant to statutory or regulatory obligation (including audit trails required by Indian law or by Customer's regulator): retained for the shorter of the legally-required retention period and seven (7) years, and destroyed thereafter.

10.5 Certification

On Customer's written request, Security Brigade shall provide written certification that destruction has been completed in accordance with this Section 10.

11. Liability

Each party's aggregate liability under this DPA is subject to and counts toward the cap set out in the MSA. Nothing in this DPA excludes or limits liability that cannot lawfully be excluded or limited under Applicable Law.

12. Miscellaneous

12.1 Conflicts

In the event of any conflict between this DPA and the MSA, this DPA prevails to the extent of the conflict in respect of the Processing of Personal Data. In the event of any conflict between this DPA and the SCCs incorporated under Section 5.1, the SCCs prevail.

12.2 Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions remain in full force and effect, and the parties shall negotiate in good faith a replacement provision that achieves the original commercial intent as closely as possible.

12.3 Governing law and jurisdiction

This DPA is governed by the laws of the Republic of India. The courts of Mumbai, Maharashtra have exclusive jurisdiction over any dispute arising out of or in connection with this DPA, save that Customer may bring proceedings in respect of data-protection matters in the courts of the data subject's habitual residence as required by mandatory provisions of Applicable Law.

12.4 Incorporation

This DPA is incorporated into the MSA by reference and forms a binding part of the agreement between the parties. Each party's signature on the MSA constitutes execution of this DPA. No separate signature page is required.

12.5 Updates

Security Brigade may update this DPA from time to time. Material changes affecting Customer rights take effect thirty (30) days after publication of the updated DPA and notification to Customer; non-material changes (typographical fixes, clarifications, Annex C updates per Section 4.2) take effect on publication.

Annex A — Subject matter, duration, nature and purpose of processing

This Annex is a template. The specific values for each engagement are set out in the applicable Statement of Work or MSA. If not separately specified, the defaults below apply.

A.1 Subject matter

Personal Data Processed in connection with the Services, including data flowing through Security Brigade's Sentinel platform and data accessed during security engagements (vulnerability assessments, penetration tests, red-team exercises, audits, incident response, and managed services).

A.2 Duration

For the term of the MSA, plus any destruction or retention periods set out in Section 10 of this DPA.

A.3 Nature and purpose

Provision of cybersecurity assessment, advisory, monitoring, and incident-response services to enable Customer to identify, manage, and remediate cybersecurity risk.

A.4 Categories of Personal Data

To the extent encountered in the course of the Services (and only such Personal Data as is necessary for the Services):

- identifiers (names, business contact details, role/title);
- authentication credentials encountered during testing (which Security Brigade does not retain except as necessary to evidence findings, and only in redacted form);
- log data, network traffic metadata, and security telemetry produced or observed during testing;
- such other categories as may be expressly identified in a Statement of Work.

Security Brigade does not require access to special categories of Personal Data (GDPR Article 9) for delivery of the Services. Where such categories may be encountered (for example, healthcare-sector engagements), additional protective measures are agreed in the Statement of Work.

A.5 Categories of data subjects

- Customer employees, contractors, and authorised users of Customer systems;
- Customer's customers and end-users whose data resides in systems within the scope of the Services;
- third parties whose data is incidentally encountered in the course of testing.

Annex B — Technical and organisational security measures

Security Brigade maintains the following technical and organisational measures, which are reviewed at least annually and updated as required.

B.1 Information security management

- ISO/IEC 27001 certified Information Security Management System.
- SOC 2 Type II attestation in progress.
- Annual external penetration test of Security Brigade's own infrastructure.
- Documented information security policies covering acceptable use, access control, cryptography, physical and environmental security, operations security, communications security, supplier relationships, incident management, and business continuity.

B.2 Personnel

- Background-verified personnel for all roles with access to Customer Personal Data.
- Mandatory annual data-protection and information-security training.
- Written confidentiality undertakings binding all personnel, contractors, and authorised testers.

B.3 Access control

- Role-based access control with least-privilege defaults.
- Multi-factor authentication required for all production systems and for access to Customer Personal Data.
- Privileged access logged and reviewed.
- Access revoked within one business day of personnel leaving or changing role.

B.4 Encryption

- Data at rest: encrypted using AES-256 or equivalent industry-standard cryptography.
- Data in transit: encrypted using TLS 1.2 or higher with strong cipher suites and certificate pinning where applicable.
- Key management: hardware security modules or cloud KMS equivalents; rotation per industry standards.

B.5 Physical and environmental security

Security Brigade operates from Tier-3+, ISO/IEC 27001 and/or SOC 2 audited colocation facilities. Current regions include Mumbai, Paris, Singapore, and Dubai. Operator names are disclosed under non-disclosure on Customer request.

B.6 Backups and resilience

- Encrypted backups stored in geographically-separated facilities with region-locking available per Customer election.
- Documented business continuity and disaster recovery plans, tested at least annually.

B.7 Logging and monitoring

- Centralised logging of access to Customer Personal Data.
- Security monitoring and alerting, including for anomalous access patterns.
- Log retention sufficient to meet statutory and regulatory requirements.

B.8 Incident response

- Documented Personal Data Breach response procedure including detection, containment, eradication, recovery, and notification.
- 24x7 incident response capability.
- Notification to affected Customers within 72 hours of becoming aware of a Personal Data Breach (Section 6).

B.9 Secure development

- Documented secure software development lifecycle for Security Brigade's own platforms (Sentinel, ShadowMap, internal tooling).
- Code review and security testing of changes affecting Customer Personal Data.

B.10 Sub-processor management

- Sub-processors listed in Annex C are bound by contractual data-protection obligations no less protective than this DPA.
- Annual review of Sub-processor security posture.

Annex C — Approved sub-processors

The following Sub-processors are engaged by Security Brigade for Processing of Customer Personal Data as of the Effective Date.

Sub-processor	Role	Region(s)
Cloudflare, Inc.	CDN, DNS, edge security, WAF	Global edge
Amazon Web Services, Inc.	Encrypted backup storage (S3)	Region-locked per Customer election
SendGrid (Twilio Inc.)	Transactional email	United States
Mailtrap	Transactional email (non-production / sandbox)	European Union
Twilio Inc.	Voice and SMS to Customer-designated contacts	United States / global
Exotel Techcom Pvt. Ltd.	Voice to Indian-jurisdiction Customer contacts	India
Microsoft Corporation	Operational email (Microsoft 365)	European Union / India
Google LLC	Operational email (Google Workspace)	European Union / India

Not sub-processors

Security Brigade operates self-hosted source control, error tracking, internal audit management, and customer relationship management systems on its own infrastructure. These are not third-party Sub-processors.

Large language model providers (including Anthropic, OpenAI, and DeepSeek) are not Sub-processors of Customer Personal Data; Security Brigade does not transmit Customer Personal Data to such providers — see Section 3.10.

Colocation operators are not Sub-processors of Customer Personal Data; they provide physical hosting and environmental security only and do not process Personal Data. Operator names and facility details are disclosed under non-disclosure on Customer request.

Background-check vendors used by Security Brigade for personnel vetting process Security Brigade employee data, not Customer Personal Data, and are therefore not Sub-processors under this DPA.

Updates

Security Brigade gives Customer at least thirty (30) days' prior notice of any addition or replacement of a Sub-processor, as set out in Section 4.2. The current Annex C is maintained at https://securitybrigade.com/legal/dpa/.

Annex D — Standard Contractual Clauses (reference)

Where transfers of Personal Data outside the EEA require Standard Contractual Clauses under Section 5.1, the parties incorporate by reference the Module Two (Controller to Processor) Standard Contractual Clauses set out in European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, the full text of which is available at:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Where transfers of Personal Data subject to the UK GDPR outside the United Kingdom require additional protection, the parties additionally incorporate the UK ICO International Data Transfer Addendum (Version B1.0, in force 21 March 2022), the full text of which is available at:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

Annex I.A (List of Parties) is populated by Annex A of this DPA. Annex I.B (Description of Transfer) is populated by Annex A of this DPA. Annex I.C (Competent Supervisory Authority) is determined per Section 5.1 of this DPA. Annex II (Technical and Organisational Measures) is populated by Annex B of this DPA. Annex III (List of Sub-processors) is populated by Annex C of this DPA.

The optional clauses of the SCCs (the Clause 7 docking clause and the Clause 11(a) independent dispute resolution option) are not selected.

End of Data Processing Agreement v1.0 · Effective 2026-01-01