Data Processing Agreement — B-52

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 subscribing to B-52 ("**Customer**", "**you**", or "**Controller**"), agree as follows.

B-52 is a product of Security Brigade InfoSec Private Limited. It is not a separate legal entity, and this DPA is entered into with Security Brigade.

1. Background and definitions

This DPA applies whenever Security Brigade Processes Personal Data on behalf of Customer in the course of providing B-52 ("**the Services**"). The Services comprise Customer's use of the B-52 agentic penetration testing platform and the security testing delivered through it, in each of the three delivery models — fully autonomous, autonomous with expert verification, and human-led — across every coverage class made available to Customer.

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 this DPA 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 Agreement 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 Agreement.
- **Customer Personal Data** means Personal Data Processed by Security Brigade on behalf of Customer under the Agreement, 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

© Security Brigade InfoSec Pvt. Ltd.

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.
- **Agreement** means the Master Services Agreement, order form, statement of work, or online subscription terms accepted by Customer, which incorporates this DPA.
- **Engagement** means a discrete authorised test run through the Services against a scope Customer has approved.
- **Engagement Material** means the scope, target-disclosed information, finding evidence, source code where in scope, and reports generated in the course of an Engagement.
- **Anonymisation Layer** means Security Brigade's anonymisation and tokenisation layer described in Section 3.10(a).
- **Model Hosting Option** means the arrangement, elected by Customer under Section 3.12, under which the large language models used to deliver the Services are hosted.
- **Services** means the B-52 platform and the security testing delivered through it, as described in Section 1.
- **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.

2.1 Data minimisation by design

The Services are designed so that Engagements do not, in the ordinary case, require access to Customer's own customers' records. An authorisation defect is proved by demonstrating a path to a single record; enumerating further records proves nothing additional. Accordingly, any action that would use a live

© Security Brigade InfoSec Pvt. Ltd.

account's credentials or read a real person's records is subject to a separate written approval by Customer before it is performed, and the report identifies every finding for which such approval was given.

This is a property of how the Services operate rather than a policy applied to them, and Customer may verify it against the audit trail for any Engagement.

2.2 Platform-improvement processing

Security Brigade is a Controller, and not a Processor, in respect of the platform-improvement processing described in Section 3.10(d), which is carried out on anonymised material for Security Brigade's own purposes. Customer's rights in respect of that processing are set out in Section 3.11.

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 Agreement, this DPA, the authorised scope of each Engagement, 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.

© Security Brigade InfoSec Pvt. Ltd.

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 Agreement, 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

The Services are delivered using large language models. Models are selected for a given task by the platform on the basis of measured performance, from among those available under Customer's Model Hosting Option, and are not allocated by coverage class. The following controls apply in every case, and each is independently auditable on request:

(a) Anonymisation and tokenisation before transmission. Security Brigade processes Engagement Material through the Anonymisation Layer before transmitting it to any third-party large language model provider engaged by Security Brigade. The Anonymisation Layer is configured to replace Customer-identifying data with randomised or tokenised values, so that the provider performs its analysis on an abstracted representation of Customer's environment. Customer-identifying data for this purpose includes domains and subdomains, application names and identifiers, internal keywords and project references, user and account identifiers, Personal Data, and other Customer-specific contextual data. The mapping between those values and Customer's data is held by Security Brigade and is not transmitted to the provider. On receipt of a response, Security Brigade maps the values back to Customer's context before the result is presented to Customer or passed to downstream tooling. Where Customer requires that no Engagement Material reach a model provider engaged by Security Brigade, Customer may elect a Model Hosting Option under Section 3.12(b), (c) or (d).

(b) Self-hosted processing of identifiable material. Where Processing requires Engagement Material in identifiable form, that Processing is performed by models operated by Security Brigade on infrastructure under its own control or, where Customer has elected a Model Hosting Option under Section 3.12(c) or (d), by the models that option provides. Models operated by Security Brigade are not third-party services, and no third party receives Personal Data in the course of Processing performed on them.

(c) No provider training. The third-party model providers identified in Annex C do not use inputs or outputs submitted through their commercial application programming interfaces to train their models, and are bound to that position by their published commercial terms. Such providers retain inputs and outputs only for a limited abuse-monitoring period determined by those terms, after which the material is deleted.

(d) Platform improvement. Security Brigade uses anonymised Engagement Material to improve the detection capability and performance of the Services. Material used for this purpose is anonymised such that it identifies neither Customer nor any Data Subject. Customer may exclude its material from this use at any time under Section 3.11.

© Security Brigade InfoSec Pvt. Ltd.

3.11 Exclusion from platform improvement

Customer may at any time, by written notice to privacy@securitybrigade.com, require that its Engagement Material be excluded from the platform-improvement use described in Section 3.10(d). Security Brigade shall give effect to that election within thirty (30) days of receipt and shall confirm it in writing.

The election is available at no charge, carries no change to fees, and has no effect on the scope, quality, or delivery of the Services. It operates prospectively: material already incorporated in anonymised form cannot be attributed to Customer and therefore cannot be retrospectively identified or withdrawn.

3.12 Model hosting

Customer elects one of the following Model Hosting Options in its order form or statement of work, or by written agreement with Security Brigade. Where no election is made, Standard Hosting applies, and Standard Hosting applies to every Service purchased through the self-service flow. Any fees for an option other than Standard Hosting are set out in the Agreement.

(a) Standard Hosting. The Services use the third-party large language model providers identified in Annex C, subject to Sections 3.10(a) and 3.10(c), together with the models Security Brigade operates under Section 3.10(b).

(b) Dedicated Hosting. The models used to deliver the Services run on compute infrastructure owned and operated by Security Brigade and allocated to Customer alone. No third-party large language model provider receives Customer's Engagement Material, and the model-provider entries in Annex C do not apply to Customer.

(c) Customer-Environment Hosting. The Services are deployed with supported large language models hosted within Customer's own environment. Model inference takes place within that environment and Customer's security boundary. No third-party large language model provider engaged by Security Brigade receives Customer's Engagement Material, and the model-provider entries in Annex C do not apply to Customer.

(d) Customer-Provided Models. The Services use a large language model provided by Customer, whether through Customer's enterprise agreement with a model provider or hosted privately by or for Customer. The model must meet Security Brigade's capability requirements for autonomous security testing and must be included in, or validated against, Security Brigade's supported model set. The provider of that model is engaged by Customer under Customer's own terms and is not a Sub-processor of Security Brigade. Security Brigade transmits Engagement Material to that model on Customer's documented instructions under Section 3.1.

The B-52 platform and its orchestration are the same under every Model Hosting Option, and Section 2.1 applies under each of them.

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.

© Security Brigade InfoSec Pvt. Ltd.

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 and data residency

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 supervisory authority of the data exporter's establishment.

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.

© Security Brigade InfoSec Pvt. Ltd.

5.4 Residency election

Customer elects the region in which its Engagement Material is stored and processed at rest. The available regions are:

- India
- European Union
- United States
- Singapore / Asia-Pacific

Security Brigade configures storage, processing at rest, and backup locations in accordance with that election. Where Customer is an entity within the scope of CERT-In Directions No. 20(3)/2022-CERT-In (issued 28 April 2022, effective 27 June 2022), which require 180 days of rolling ICT logs to be maintained within Indian jurisdiction, the India election is available for that purpose.

5.5 Model inference and the residency election

Customer's residency election governs where Engagement Material is stored and processed at rest. It does not govern where model inference occurs, which is determined by Customer's Model Hosting Option under Section 3.12:

- **Standard Hosting.** Inference performed by models operated by Security Brigade on its own infrastructure, as described in Section 3.10(b), takes place within Security Brigade's own environment. Inference performed by the third-party providers identified in Annex C may take place outside Customer's elected region, including in the United States. Material transmitted to those providers has first been processed through the Anonymisation Layer, as set out in Section 3.10(a), and the providers do not train their models on it, as set out in Section 3.10(c).
- **Dedicated Hosting.** Inference takes place on infrastructure owned and operated by Security Brigade and allocated to Customer.
- **Customer-Environment Hosting.** Inference takes place within Customer's own environment.
- **Customer-Provided Models.** Inference takes place wherever Customer's model is hosted, as determined by Customer and its provider.

Where Customer requires model inference to remain within a boundary it defines, Customer-Environment Hosting and Customer-Provided Models place that decision with Customer.

This Section is stated expressly so that Customer's assessment of its own regulatory position is made on complete information.

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:

© Security Brigade InfoSec Pvt. Ltd.

- 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 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,

© Security Brigade InfoSec Pvt. Ltd.

in each case to the extent the assessment or consultation relates to Personal Data Processed by Security Brigade under the Agreement, 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 and certifications

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
- evidence of Security Brigade's CERT-In empanelment.

These are instruments held by Security Brigade in respect of its delivery of security services. They are not certifications of the B-52 platform itself.

9.2 Engagement audit trail

In addition to the reports in Section 9.1, Customer may at any time inspect the audit trail for any of its own Engagements, which records the authorised scope, the actions taken, and each approval given under Section 2.1.

9.3 On-site inspection

Where the reports in Sections 9.1 and 9.2 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 Agreement;
- 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.

9.4 Post-breach inspection

The frequency limit in Section 9.3 does not apply to an inspection conducted following a Personal Data Breach, which may be conducted on shorter notice reasonable in the circumstances.

© Security Brigade InfoSec Pvt. Ltd.

10. Term, retention, 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 Agreement.

10.2 Retention during the term

Security Brigade retains Engagement Material as follows:

Material	Retention
Source code, where a review is in scope	Deleted after thirty (30) days of Engagement inactivity
Scope records, finding evidence, target-disclosed information, and reports	Retained for the duration of the Engagement and for twelve (12) months thereafter, then deleted
Credentials issued by Customer for testing	Not retained beyond the Engagement; Customer is responsible for revoking them
Platform account and billing records	Retained for the term of the Agreement and thereafter as set out in Section 10.5

Where a source-code review runs inside Customer's own pipeline, the source code does not leave that pipeline and is not retained by Security Brigade at all.

Customer may request deletion of any Engagement Material earlier than the periods above, and Security Brigade shall give effect to that request within thirty (30) days, subject to Section 10.5.

10.3 Destruction by default

On termination or expiry of the Agreement, Security Brigade shall destroy all Customer Personal Data in its possession or control, including any backups and archived copies, subject to Section 10.5 (statutory retention).

10.4 Customer-elected return

Customer may, by written notice given prior to or within thirty (30) days after termination or expiry of the Agreement, 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, 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 10.5.

10.5 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;

© Security Brigade InfoSec Pvt. Ltd.

- 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.

10.6 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 Agreement. 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 Agreement, 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 and execution

This DPA is incorporated into the Agreement by reference and forms a binding part of it.

Where Customer has entered into a Master Services Agreement or order form, that party's signature on it constitutes execution of this DPA and no separate signature page is required. Where Customer has subscribed to the Services through the self-service flow, Customer's acceptance of the online subscription terms at the point of purchase constitutes acceptance of this DPA. In either case this DPA applies in full and on identical terms.

A countersigned copy of this DPA is available to any Customer on written request to privacy@securitybrigade.com.

© Security Brigade InfoSec Pvt. Ltd.

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

A.1 Subject matter

Personal Data Processed in connection with Customer's use of the B-52 platform and the Engagements run through it.

A.2 Duration

For the term of the Agreement, plus the retention and destruction periods set out in Section 10.

A.3 Nature and purpose

Provision of automated and expert-verified penetration testing to enable Customer to identify, evidence, and remediate security defects in systems Customer owns or is authorised to test.

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 them:

Platform account data — the names, business email addresses, and roles of Customer personnel who use the platform, and Customer's billing contact details.

Engagement Material — the categories below, which describe Customer's systems rather than Customer's own customers:

- the authorised scope: targets, coverage classes, roles, and where applicable the movement boundary;
- information disclosed by the targets themselves: software versions, configuration, routes, and comparable material returned by discovery;
- the evidence for each finding: the request as sent and the response as returned, with the portion evidencing the defect marked;
- source code, where a source-code review is within the authorised scope;
- credentials issued by Customer for the purpose of the Engagement.

Personal Data belonging to Customer's own customers or end users is not, in the ordinary case, Processed at all: any action that would read a real person's records requires Customer's separate written approval under Section 2.1, and the report identifies every finding for which such approval was given.

A.5 Categories of Data Subjects

- Customer personnel who hold platform accounts;
- Customer personnel identified in target-disclosed information;
- where and only where Customer has given approval under Section 2.1, the individuals whose records were read in evidencing a specific finding.

© Security Brigade InfoSec Pvt. Ltd.

A.6 Special categories

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, in an Engagement against a healthcare system — additional protective measures are agreed before the Engagement begins.

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.
- CERT-In empanelment.
- 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.
- 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 audited facilities in each region offered under Section 5.4. Operator names and facility details are disclosed under non-disclosure on Customer request.

B.6 Backups and resilience

- Encrypted backups stored in geographically-separated facilities within Customer's elected region.
- Documented business continuity and disaster recovery plans, tested at least annually.

© Security Brigade InfoSec Pvt. Ltd.

B.7 Logging and monitoring

- Centralised logging of access to Customer Personal Data.
- Security monitoring and alerting, including for anomalous access patterns.
- A per-Engagement audit trail available to Customer under Section 9.2.
- Log retention sufficient to meet statutory and regulatory requirements, including 180 days of rolling ICT logs within Indian jurisdiction where the India region is elected.

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 Autonomy and approval controls

- Any action that would use a live account's credentials or read a real person's records is gated behind Customer's separate written approval (Section 2.1).
- Testing is bounded by the scope Customer authorises, and the audit trail records the scope against which each Engagement was run.
- Anonymisation and tokenisation of Engagement Material before transmission to any third-party model provider engaged by Security Brigade (Section 3.10(a)).
- A choice of Model Hosting Option, including options under which no third-party model provider engaged by Security Brigade receives Engagement Material (Section 3.12).

B.10 Secure development

- Documented secure software development lifecycle for the B-52 platform.
- Code review and security testing of changes affecting Customer Personal Data.

B.11 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 in connection with the Services as of the Effective Date. The two large language model providers apply only where Customer uses Standard Hosting under Section 3.12(a).

© Security Brigade InfoSec Pvt. Ltd.

Sub-processor	Role	Region(s)
Cloudflare, Inc.	CDN, DNS, edge security, WAF	Global edge
Amazon Web Services, Inc.	Encrypted backup storage	Region-locked per Customer election
Anthropic PBC	Large language model inference — Standard Hosting only; input processed through the Anonymisation Layer, per Section 3.10(a)	United States
OpenAI, L.L.C.	Large language model inference — Standard Hosting only; input processed through the Anonymisation Layer, per Section 3.10(a)	United States
Stripe, Inc.	Subscription and card payment processing	United States / European Union
Razorpay Software Private Limited	Subscription and card payment processing	India
SendGrid (Twilio Inc.)	Transactional email	United States
Microsoft Corporation	Operational email (Microsoft 365)	European Union / India
Google LLC	Operational email (Google Workspace)	European Union / India

Not sub-processors

Large language models operated by Security Brigade on infrastructure under its own control, including infrastructure allocated to Customer under Dedicated Hosting (Section 3.12(b)), are not Sub-processors. No third party receives Customer Personal Data in the course of that Processing, and the models are run by Security Brigade rather than accessed as a third-party service — see Section 3.10(b).

The third-party model providers listed in the table above are identified in the interest of transparency. They are used only under Standard Hosting, they receive Engagement Material only after it has been processed through the Anonymisation Layer, as set out in Section 3.10(a), and they do not train their models on it, as set out in Section 3.10(c).

Models hosted within Customer's own environment under Customer-Environment Hosting (Section 3.12(c)) are not Sub-processors of Security Brigade. Where Customer elects Customer-Provided Models (Section 3.12(d)), the provider of that model is engaged by Customer under Customer's own terms and is not a Sub-processor of Security Brigade.

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

Colocation operators are not Sub-processors of Customer Personal Data. They provide physical hosting and environmental security only, have no logical access to Customer Personal Data, and do not Process it. This applies to the facilities serving every region offered under Section 5.4, including the United States. Operator names and facility details for any region are disclosed under non-disclosure on Customer request.

© Security Brigade InfoSec Pvt. Ltd.

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://b52security.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 B-52 Data Processing Agreement v1.1 · Effective 2026-09-16 · Last updated 2026-10-01

© Security Brigade InfoSec Pvt. Ltd.