

BumbleB Data Processing Agreement

Version 2026.3 · Effective 10 October 2026 · Last updated 9 October 2026

1. Parties, scope and precedence

1.1 This Data Processing Agreement ("DPA") is between the BumbleB entity named in the Terms of Service or the Order Form — by default **BumbleB Technologies Pvt Ltd** ("BumbleB") — and the customer that has agreed to BumbleB's Terms of Service ("Customer").

1.2 This DPA forms part of the Terms of Service for every Customer, on paid plans, free plans and free trials alike. It applies without signature. A copy signed by BumbleB is available as a PDF at <https://bumbleb.co/legal/dpa.pdf> for Customers whose procurement process requires one.

1.3 This DPA applies whenever BumbleB processes Customer Personal Data in providing the Service. It does not govern Account Data or Usage Data, which BumbleB processes for its own purposes as described in the Privacy Policy, except where this DPA says otherwise.

1.4 On data-protection matters, this DPA prevails over the Terms of Service and the Order Form, unless an Order Form expressly says that it overrides a specific clause of this DPA. Where the Standard Contractual Clauses apply, they prevail over this DPA to the extent of any conflict. A regional annex prevails over the rest of this DPA for processing within its scope.

2. Definitions

2.1 Capitalised terms not defined in this DPA have the meaning given in the Terms of Service. In this DPA:

- **"Customer Content"** means Inputs, Outputs and Visitor Data.
- **"Inputs"** means what Customer or its Users type, upload or connect to the Service.
- **"Outputs"** means what the Service writes back: answers, explanations, charts, tables and generated queries.
- **"Visitor Data"** means what the tracking tag collects about visitors to Customer's websites.
- **"Account Data"** means information about who Customer and its Users are and how they use the account, such as users, logins, seats, plan, invoices, payments, feature-level activity counts, support tickets and call notes.
- **"Usage Data"** means BumbleB's identity-free record of how the Service ran: which tools were called and in what order, the types (never the values) of their arguments, the category of the request, errors, retries, timing, and whether the answer was accepted.
- **"Submitted Conversation"** means a conversation a User chooses to send to BumbleB, for example by selecting "Report a bug".
- **"Feedback"** means suggestions and ideas about the Service. Feedback does not include a Submitted Conversation.
- **"User"** means an individual whom Customer permits to use the Service under its account.
- **"Personal Data"** means any information relating to an identified or identifiable individual, and includes "personal information" and "personal data" as defined in Data Protection Laws.
- **"Customer Personal Data"** means Personal Data contained in Customer Content.

- **"Data Subject"** means the individual to whom Personal Data relates, and includes a "Data Principal" under the DPDP Act and a "consumer" under US state privacy laws.
- **"Controller"** means the party that determines the purposes and means of processing, and includes a "Data Fiduciary" under the DPDP Act and a "business" or "controller" under US state privacy laws.
- **"Processor"** means the party that processes Personal Data on behalf of a Controller, and includes a "Data Processor" under the DPDP Act and a "service provider" or "processor" under US state privacy laws.
- **"Sub-processor"** means a third party engaged by BumbleB to process Customer Personal Data.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data processed by BumbleB or its Sub-processors.
- **"Data Protection Laws"** means all laws on privacy and Personal Data that apply to a party's processing under the Agreement, including India's Digital Personal Data Protection Act 2023 and its Rules (the "DPDP Act"), the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR as it forms part of UK law ("UK GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act and its regulations ("CCPA"), and other US state privacy laws.
- **"Standard Contractual Clauses"** means the clauses annexed to European Commission Implementing Decision (EU) 2021/914, and **"UK Addendum"** means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.
- **"Order Form"** has the meaning in the Terms of Service.
- **"Enterprise plan"** means a plan sold under an Order Form designated Enterprise.
- **"Agreement"** means the Terms of Service, any Order Form and this DPA.

3. Roles and instructions

3.1 Roles. For Customer Personal Data, Customer is the Controller and BumbleB is the Processor. Where Customer is itself a Processor for another Controller, BumbleB is Customer's Sub-processor and Customer is responsible for obtaining that Controller's authorisation for this DPA.

3.2 Instructions. BumbleB processes Customer Personal Data only on Customer's documented instructions, unless the law that applies to BumbleB requires otherwise, in which case BumbleB will tell Customer before processing unless that law prohibits it. The Agreement, Customer's configuration of the Service, and Customer's use of its features are Customer's complete documented instructions at the effective date. Further instructions must be consistent with the Agreement.

3.3 Unlawful instructions. BumbleB will tell Customer promptly if, in its opinion, an instruction infringes Data Protection Laws, and may decline to follow that instruction until Customer confirms or changes it.

3.4 Customer responsibilities. Customer is responsible for the lawfulness of the Customer Personal Data it provides or collects through the Service, for having a lawful basis or valid consent for that processing, and for giving Data Subjects the notices that Data Protection Laws require.

3.5 Details of processing. The subject matter, duration, nature and purpose of the processing, and the types of Personal Data and categories of Data Subjects, are set out in Annex 1.

4. Customer Content and Usage Data

4.1 No training. BumbleB will not use Customer Content to train, retrain or fine-tune any AI model, and will not allow any sub-processor to do so. The only exception is a Submitted Conversation, which a user chooses to send to BumbleB.

4.2 Usage Data. BumbleB records how the Service runs — which tools were called, in what order, and whether they worked — without names, account identifiers or the values in Customer's data. BumbleB uses Usage Data only to operate, secure, measure and improve the Service.

4.3 No human reading. BumbleB staff do not read Customer Content to improve the Service. Staff read it only to provide support Customer asks for, to investigate security or abuse, or when a User sends a conversation to BumbleB as a Submitted Conversation.

4.4 Authorisation to create Usage Data. Customer authorises and instructs BumbleB to create Usage Data from Customer's use of the Service. In creating Usage Data, BumbleB will:

- (a) record it without user, account, session or message identifiers;
- (b) replace every argument value with a placeholder describing only its type, at the moment of recording;
- (c) record no free text, including no questions, answers, queries, column names, result values or model reasoning;
- (d) use it only to operate, secure, measure and improve the Service, including to train BumbleB's own service components, such as the components that choose which tool to call. Usage Data is the only data derived from Customer Content that BumbleB uses to train anything;
- (e) never sell it, share it or give it to any third party for that party's own purposes; and
- (f) never link it, or attempt to link it, back to Customer, a User, a Data Subject or a session.

4.5 Automated quality checks. While a session runs, BumbleB may use automated processes to assign the request a category from a fixed list and to compare the request with the steps the Service took, recording only a verdict from a fixed list. Within 90 days of a session, BumbleB may use automated processes to re-check that session in order to add a new category or verdict. Re-checks exclude Visitor Data. These processes output labels and verdicts only. No person reads session content for this purpose, and no text from the session is copied into Usage Data.

4.6 Submitted Conversations. Customer authorises its Users to send a conversation to BumbleB as a Submitted Conversation. A Submitted Conversation exists only because a User chose to send it, after being shown how BumbleB will use it. BumbleB may read a Submitted Conversation and use it to improve the Service, including to train its own models. Before any person at BumbleB reads it, BumbleB masks any Visitor Data it contains. A User or Customer may withdraw a Submitted Conversation at any time, after which BumbleB will delete it and stop using it; a model already trained using it is not retrained. BumbleB keeps a Submitted Conversation for 12 months from submission, or until it is withdrawn if sooner. Customer's administrators may turn off Submitted

Conversations for Customer's workspace at any time; they are off by default on Enterprise plans. While they are off, no User can send one.

4.7 Support. When Customer asks for support, BumbleB staff may read the relevant session where it is stored, under Section 6.2. Nothing read for support is copied into Usage Data, evaluation sets or training data.

4.8 Visitor Data. BumbleB will never use Visitor Data to improve the Service, under any setting or configuration, including within a Submitted Conversation. Usage Data may describe a session that queried Visitor Data, such as which tools ran, but never contains Visitor Data.

4.9 No profiling. BumbleB will not build profiles of individual Users or Data Subjects to change how the Service behaves for them, and will not link an individual's activity across sessions for that purpose.

4.10 Sales and account management. BumbleB's sales and customer-success staff use Account Data only. They see which features an account uses and how much, never what was asked or answered.

4.11 After termination. Usage Data identifies no one, so it is not returned or deleted when the Agreement ends and BumbleB may keep it for as long as it is useful. Section 4.4 continues to apply to it.

4.12 Objections. Where Data Protection Laws give a Data Subject the right to object to the creation of Usage Data from their sessions, BumbleB will honour a valid objection passed to it by Customer or received directly, and will stop creating Usage Data from that Data Subject's sessions where it can identify them.

5. The tracking tag

5.1 Customer's responsibilities. For each website on which Customer installs the tracking tag, Customer is responsible for: obtaining any consent that Data Protection Laws or cookie laws require for the tag; operating a compliant consent banner where one is required; having a lawful basis for the Visitor Data the tag collects; and giving visitors the required privacy notice.

5.2 BumbleB's responsibilities. BumbleB processes only what Customer's configuration of the tag transmits, and only for websites Customer has verified with BumbleB. The tag honours consent signals at the point of collection, including Global Privacy Control and equivalent signals that Customer configures the tag to respect.

5.3 Activation and separation. Before the tag is activated, BumbleB requires Customer to verify control of the domain and to acknowledge its responsibilities under Section 5.1. Visitor Data is kept separate for each verified website, and Customer may delete the Visitor Data for one website without affecting others.

5.4 Children. Customer will not install the tag on a website or service directed at children under 18. If BumbleB learns that a tagged website is so directed, it may stop collection for that website and delete its Visitor Data, and will tell Customer.

6. Confidentiality and staff access

6.1 Confidentiality. BumbleB ensures that every person it authorises to process Customer Personal Data is bound by a duty of confidentiality and accesses that data only as needed for the purposes in this DPA.

6.2 Access to Customer Content. Staff access to Customer Content is limited to named support, on-call and security roles. Each access must be linked to a support ticket or security incident, is logged with who accessed what, when and why, and is read where the data is stored rather than copied. On request, BumbleB will tell Customer whether and under which ticket its sessions were accessed.

7. Security

7.1 BumbleB implements and maintains appropriate technical and organisational measures to protect Customer Personal Data against Personal Data Breaches, taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing and the risks to Data Subjects. The current measures are described in Annex 2.

7.2 BumbleB may update its security measures over time, provided the updates do not materially reduce the overall protection of Customer Personal Data.

8. Sub-processors

8.1 General authorisation. Customer gives BumbleB general authorisation to engage Sub-processors. The current Sub-processors are listed in the [sub-processor list](#) referred to in Annex 3.

8.2 Notice of changes. BumbleB will give at least 30 days' notice before adding or replacing a Sub-processor, by updating the sub-processor list and notifying Customers who have subscribed to changes and the account's administrators by email.

8.3 Emergency replacement. If a Sub-processor suffers a security incident, becomes insolvent, or stops providing its service, BumbleB may replace it with less than 30 days' notice where that is needed to keep the Service running or Customer Personal Data secure. BumbleB will give notice as soon as practicable and in any case within 5 business days, and Customer's rights under Section 8.4 apply in the same way.

8.4 Objection. Customer may object to a new Sub-processor on reasonable data-protection grounds by writing to BumbleB within the notice period. The parties will discuss the objection in good faith, and BumbleB may offer a way to provide the Service without that Sub-processor processing Customer Personal Data. If the objection is not resolved within 30 days, Customer may terminate the affected Service by written notice, and BumbleB will refund any prepaid fees for the period after termination.

8.5 Flow-down. BumbleB will engage each Sub-processor under a written contract that imposes data protection obligations no less protective than this DPA, including a prohibition on training any model on Customer Content and on using Customer Personal Data for the Sub-processor's own purposes. BumbleB remains liable to Customer for each Sub-processor's performance of those obligations.

8.6 AI model providers. Sub-processors that provide AI models receive Customer Content only to generate Outputs (inference). Their retention terms, including any retention for abuse monitoring, are stated on the sub-processor list.

9. Assistance with Data Subject requests

9.1 Taking into account the nature of the processing, BumbleB will assist Customer, by appropriate technical and organisational measures, to respond to requests from Data Subjects to exercise their rights under Data Protection Laws, including rights to access, correct, erase, port, restrict or object, and rights to opt out.

9.2 Customer can perform many requests itself through the Service, including deleting the Visitor Data for a specific website. Where it cannot, BumbleB will act on Customer's request in time for Customer to meet its statutory deadline.

9.3 If BumbleB receives a request directly from a Data Subject about Customer Personal Data, it will pass the request to Customer without undue delay and will not respond to it except on Customer's instruction or as the law requires.

10. Personal Data Breach

10.1 BumbleB will notify Customer without undue delay, and in any case within 24 hours, of becoming aware of a Personal Data Breach.

10.2 The notice will describe, as far as then known: the nature of the breach, including the categories and approximate number of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address it and reduce its effects; and a contact point for more information. Where not all of this is known at first, BumbleB will provide it in stages as it becomes available.

10.3 BumbleB will take reasonable steps to contain and investigate the breach and will cooperate with Customer so that Customer can meet its own obligations to notify regulators and Data Subjects. BumbleB will not notify regulators or Data Subjects on Customer's behalf unless Customer instructs it to or the law requires it.

10.4 Notifying Customer of a Personal Data Breach is not an admission of fault or liability.

11. Impact assessments and consultation

11.1 Taking into account the nature of the processing and the information available to it, BumbleB will give Customer reasonable assistance with any data protection impact assessment, and any prior consultation with a regulator, that Data Protection Laws require of Customer for its use of the Service.

12. International transfers

12.1 **Location.** BumbleB hosts Customer Content in Microsoft Azure and MongoDB Atlas, in the United States (Azure East US and East US 2). Some Sub-processors process Customer Personal Data

in other countries, as shown on the sub-processor list.

12.2 EU and UK transfers. For any Customer Personal Data that is subject to the GDPR or the UK GDPR and is transferred to BumbleB or onward to a Sub-processor in a country without an adequacy decision, the Standard Contractual Clauses (Module 2 where Customer is a Controller, Module 3 where Customer is a Processor) and the UK Addendum are incorporated into this DPA by reference. Annexes 1 to 4 of this DPA provide the information required by Annexes I, II and III of the Standard Contractual Clauses and the tables of the UK Addendum.

12.3 Onward transfers. BumbleB will make onward transfers of Customer Personal Data to Sub-processors only under a transfer mechanism recognised by Data Protection Laws, such as the Standard Contractual Clauses, and will assess the laws of the destination country where Data Protection Laws require it.

12.4 Other transfers. Transfers of Customer Personal Data subject to the DPDP Act are governed by the India annex. BumbleB will comply with any other transfer requirement of Data Protection Laws that applies to it as Processor.

12.5 Government and law-enforcement requests. If a government authority or law-enforcement agency asks BumbleB to disclose Customer Personal Data, BumbleB will:

- (a) redirect the authority to request the data directly from Customer, where possible;
- (b) notify Customer of the request promptly, unless the law prohibits it;
- (c) disclose only the minimum Customer Personal Data the law requires; and
- (d) challenge any request that it reasonably believes is unlawful.

13. Audits and information

13.1 Information. BumbleB will make available to Customer the information reasonably necessary to demonstrate its compliance with this DPA and Data Protection Laws, and will keep records of its processing as Data Protection Laws require.

13.2 Reports first. BumbleB will first meet an audit request by providing its current third-party audit reports or certifications, if any, and by answering Customer's reasonable security and privacy questionnaires.

13.3 Customer audit. If those are not enough to demonstrate compliance, if BumbleB holds no current third-party audit report, or if a regulator requires it, Customer may audit BumbleB's compliance with this DPA, itself or through an independent auditor bound by confidentiality who is not a competitor of BumbleB. An audit may take place no more than once in any 12 months, unless it follows a Personal Data Breach or a regulator requires it.

13.4 Conduct. Customer will give at least 30 days' written notice, agree the scope with BumbleB in advance, and conduct the audit during business hours without unreasonable disruption. An audit will not include access to other customers' data or to systems that do not process Customer Personal Data. Each party bears its own costs, except that BumbleB bears its own costs of an audit that follows a Personal Data Breach at BumbleB or that finds material non-compliance.

14. Retention, deletion and return

14.1 Retention. BumbleB keeps data covered by this DPA for the following periods, unless the law requires it to keep data longer:

Data	Kept for
Conversations — Inputs and Outputs in a session	90 days, then deleted; backup copies within a further 90 days
Other Customer Content, including uploaded files, connected data and Visitor Data	The term of the Agreement, or until Customer deletes it
Records of staff and user access and security events (no Customer Content)	12 months
Submitted Conversations	12 months from submission, or until withdrawn
Prompts held by AI model Sub-processors	OpenAI: up to 30 days for abuse monitoring under its terms. Through OpenRouter: not stored (zero retention), apart from brief retention a provider must keep by law
Usage Data	As long as it is useful; it identifies no one (Section 4.11)

Account Data is governed by the Privacy Policy and kept for the life of the account plus any period the law requires.

14.2 Return. On termination of the Agreement, Customer may export its Customer Content through the Service or ask BumbleB to return it. BumbleB will make it available for 30 days after termination.

14.3 Deletion. After that 30-day period, BumbleB will delete Customer Content from its active systems within a further 30 days, and from backups within 90 days. BumbleB will give Customer a written certificate of deletion on request.

14.4 Legal hold. If the law requires BumbleB to keep any Customer Content longer, or it is needed for an active legal claim, BumbleB will keep only what is required, protect it under this DPA, process it only for that purpose, and tell Customer unless the law prohibits it.

15. Regional terms

15.1 The regional annexes to this DPA add terms for India and the United States. Each applies to processing within its scope, in addition to the rest of this DPA.

16. Liability, term and changes

16.1 Liability. Each party's liability under this DPA is subject to the limitation of liability in the Terms of Service, except where Data Protection Laws or the Standard Contractual Clauses do not permit that limitation. Nothing in this DPA limits the rights of Data Subjects under the Standard Contractual Clauses.

16.2 Term. This DPA applies for as long as BumbleB processes Customer Personal Data under the Agreement, and Sections 4.11 and 14 continue after it ends.

16.3 Changes. BumbleB will give Customer at least 30 days' notice, by email and in the Service, of any material change to this DPA. A change is material if it reduces Customer's rights or expands how BumbleB uses data. BumbleB may make changes required by Data Protection Laws or a regulator on shorter notice where needed to comply. Previous versions are archived and linked from the top of this DPA.

16.4 Governing law. This DPA is governed by the law and dispute-resolution terms of the Terms of Service, except that the Standard Contractual Clauses and the UK Addendum are governed as set out in Annex 4.

17. Contacts

- **Legal and contracts:** legal@bumbleb.co
 - **Privacy:** privacy@bumbleb.co
 - **Security and breach reports:** security@bumbleb.co
 - **Grievance Officer (India):** Chinmaya Reddy, grievance@bumbleb.co
 - **Post:** the BumbleB entity named in the Terms of Service or the Order Form — by default BumbleB Technologies Pvt Ltd, 581, Second Floor, 1st Main Rd, Sector 6, HSR Layout, Bengaluru, Karnataka 560102, India
-

Annex 1 — Details of processing

Parties

- **Customer (data exporter):** the Customer named in the Order Form or account, acting as Controller (or as Processor for another Controller). Contact: the account's administrator.
- **BumbleB (data importer):** the BumbleB entity named in the Terms of Service or the Order Form — by default BumbleB Technologies Pvt Ltd, 581, Second Floor, 1st Main Rd, Sector 6, HSR Layout, Bengaluru, Karnataka 560102, India — acting as Processor. Contact: privacy@bumbleb.co.

Subject matter. Providing BumbleB's analytics Service to Customer, including operating the tracking tag on Customer's verified websites on Customer's behalf.

Duration. The term of the Agreement, plus the retention periods in Section 14.

Nature and purpose. Collecting Visitor Data through the tracking tag; storing Customer Content; analysing Inputs and generating Outputs, including by sending Inputs to AI model Sub-processors for inference; keeping the Service secure and preventing abuse; providing support Customer asks for; and creating Usage Data as described in Section 4.4.

Frequency of transfer. Continuous, for as long as Customer uses the Service.

Categories of Data Subjects

- Visitors to Customer's websites whose data the tracking tag collects.
- Customer's Users.

- Customer's own customers, prospects and other individuals whose data Customer uploads, connects or asks about.

Types of Personal Data

- **Visitor Data:** page views, clicks, custom events and sessions, with the identifiers that make them personal, such as IP address, cookie and device identifiers, browser and device details, referrer and page URL.
- **Inputs:** questions and instructions typed by Users, and any Personal Data in files or data sources Customer uploads or connects, such as names, email addresses and product activity of Customer's own customers.
- **Outputs:** any Personal Data that appears in answers, charts, tables and generated queries.
- **User identifiers** attached to Customer Content, such as name and email address.

Special categories. None intended. Customer will not use the Service to process special categories of Personal Data, sensitive personal information, or data about children, unless BumbleB agrees in writing.

Retention. As set out in Section 14.

Sub-processors. As set out in Annex 3, for the subject matter, nature and duration described in this Annex.

Annex 2 — Security measures

1. **Encryption.** Data encrypted in transit using TLS 1.2 or higher, and at rest using AES-256 or equivalent.
2. **Access control.** Role-based access on the principle of least privilege; single sign-on and multi-factor authentication for staff access to production systems; access reviewed regularly and removed promptly when no longer needed.
3. **Logging of staff access.** Every staff access to Customer Content is logged with who, what, when and why. Access logs contain no Customer Content and are kept for 12 months.
4. **Support access.** Support staff read Customer Content in place, only against a support ticket or security incident, and cannot export it to other systems.
5. **Separation.** Customer Content is separated logically by customer, and Visitor Data by verified website. Usage Data is stored apart from Customer Content and from billing records.
6. **Staff.** Background checks where lawful, confidentiality undertakings, and security and privacy training on joining and at least once a year.
7. **Secure development and vulnerability management.** Code review, dependency scanning, regular patching, and periodic security testing of the Service.
8. **Monitoring.** Monitoring and alerting for unusual activity on production systems.
9. **Backups and resilience.** Encrypted backups, tested restoration, and hosting in a region with redundant infrastructure.
10. **Incident response.** A documented incident response plan, with roles, escalation and the customer notification commitment in Section 10.
11. **Sub-processor diligence.** Security and privacy review of each Sub-processor before engagement and periodically after, with contract terms as described in Section 8.5.

12. **Deletion.** Automated deletion of conversations after 90 days and of other data on the schedule in Section 14.

Annex 3 — Sub-processors

The Sub-processors Customer authorises at the effective date, with each one's purpose, the data it receives, its location and its retention and training terms, are listed on the sub-processor list. That list forms part of this Annex and is updated under Section 8.

Annex 4 — EU and UK transfer terms

This Annex applies when the Standard Contractual Clauses or the UK Addendum apply under Section 12.2.

Standard Contractual Clauses

1. **Modules.** Module 2 (controller to processor) applies where Customer is a Controller. Module 3 (processor to processor) applies where Customer is a Processor.
2. **Clause 7 (docking clause).** The optional docking clause applies.
3. **Clause 9(a) (sub-processors).** Option 2, general written authorisation, applies. The time period for notice of changes is 30 days, as set out in Section 8.
4. **Clause 11(a) (redress).** The optional language does not apply.
5. **Clause 13 (supervision).** Where Customer is established in the EU, the competent supervisory authority is the one for Customer's establishment. Where Customer is not established in the EU but has appointed a representative under Article 27 GDPR, it is the authority of the Member State where the representative is established. Otherwise, it is the authority of the Member State in which the Data Subjects whose Personal Data is transferred are located.
6. **Clause 17 (governing law).** The law of Ireland.
7. **Clause 18 (forum).** The courts of Ireland.
8. **Annex I.A and I.B** are completed by Annex 1 of this DPA; **Annex I.C** by paragraph 5 above; **Annex II** by Annex 2; and **Annex III** by Annex 3.
9. **Instructions, deletion and audit.** Customer's instructions under Clause 8.1, the deletion certificate under Clause 8.5 and the audits under Clause 8.9 are given and carried out as set out in Sections 3, 14 and 13 of this DPA, to the extent consistent with the Standard Contractual Clauses.

UK Addendum

1. **Table 1 (parties)** is completed by Annex 1 of this DPA.
2. **Table 2 (selected SCCs)** refers to the Modules and options selected above.
3. **Table 3 (appendix information)** is completed by Annexes 1, 2 and 3 of this DPA.
4. **Table 4 (ending the Addendum):** either party may end the UK Addendum as allowed by its Section 19.

Annex — India (DPDP Act 2023)

1. Scope. This annex applies to Customer Personal Data whose processing is subject to the Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025 (the "DPDP Act"). In this annex, "Data Principal", "Data Fiduciary", "Data Processor", "Board" and "Consent Manager" have the meanings given in the DPDP Act.

2. Roles. Customer is the Data Fiduciary and BumbleB is the Data Processor for Customer Personal Data. BumbleB processes Customer Personal Data on Customer's behalf only under this contract, as section 8 of the DPDP Act requires, and only on Customer's documented instructions as set out in Section 3 of this DPA.

3. Instruction to derive Usage Data. The Customer instructs BumbleB to derive Usage Data from its use of the Service for the purpose of improving the Service. BumbleB will do so only as described in Section 4.4 of this DPA.

4. Customer's responsibilities. Customer is responsible for giving Data Principals the notice the DPDP Act requires, itemising each purpose; for obtaining and recording valid consent, or relying on another lawful ground under the DPDP Act; for handling withdrawals of consent; and, where it uses one, for its arrangements with a Consent Manager. When a Data Principal withdraws consent, Customer will tell BumbleB, and BumbleB will stop processing the affected Customer Personal Data within a reasonable time.

5. Data Principal rights. BumbleB will assist Customer, by appropriate technical and organisational measures, to meet Data Principals' rights to access information about their Personal Data, and to correction, completion, updating and erasure. In particular, BumbleB will:

- (a) act on Customer's instructions to correct or erase Customer Personal Data in time for Customer to meet its deadlines under the DPDP Act;
- (b) give Customer the information it needs to resolve grievances through its own grievance redressal mechanism within the period the DPDP Act requires; and
- (c) act on instructions from a person nominated by a Data Principal under section 14 of the DPDP Act, when Customer confirms the nomination to BumbleB.

6. Personal Data Breach. BumbleB will intimate a Personal Data Breach to Customer without delay, and in any case within 24 hours of becoming aware of it under Section 10 of this DPA, so that Customer can intimate it to the Board and to each affected Data Principal. BumbleB will give Customer a detailed report within 48 hours of becoming aware of the breach, covering the facts and circumstances, the events that led to it, the measures taken or proposed to reduce risk, the findings about the person who caused it where known, and the remedial steps taken to prevent a recurrence. BumbleB will provide information in stages before then as it becomes available.

7. Erasure. BumbleB will erase Customer Personal Data when Customer instructs it to, when Customer tells BumbleB that the specified purpose is no longer being served or that consent has been withdrawn, and in any case at the end of the Agreement under Section 14 of this DPA, unless retention is required by law. BumbleB will also cause its Sub-processors to erase it.

8. Logs. BumbleB keeps records of access to and processing of Customer Personal Data, without Customer Content, for 12 months, and will make them available to Customer where Customer needs them to meet its own obligations under the DPDP Act.

9. Children. Customer will not use the Service to process the Personal Data of children, or to track or monitor the behaviour of children, in a way that the DPDP Act prohibits. Section 5.4 of this DPA applies to websites directed at children. Where Customer obtains verifiable consent of a parent or lawful guardian for any processing, Customer is responsible for it.

10. Significant Data Fiduciaries. If Customer is notified as a Significant Data Fiduciary, BumbleB will give Customer reasonable assistance with its data protection impact assessments and audits under Section 11 and Section 13 of this DPA.

11. Transfers outside India. BumbleB hosts Customer Content in the United States. Transfers of Customer Personal Data outside India, including to the Sub-processors listed on the sub-processor list, are made under the DPDP Act, which permits transfers except to countries the Central Government restricts by notification. At the effective date no country has been so restricted. If a country where a Sub-processor processes Customer Personal Data is restricted, BumbleB will stop transferring Customer Personal Data there and will tell Customer. The Service does not offer hosting in India. Customer must not use the Service for personal data that a law or sector-specific requirement obliges it to keep in India.

12. Customer's liability. Customer remains responsible as Data Fiduciary for complying with the DPDP Act for processing undertaken on its behalf by BumbleB, as section 8(1) of the DPDP Act provides. This annex does not shift that responsibility to BumbleB, and does not limit BumbleB's liability to Customer under the Agreement for BumbleB's own breach of this DPA.

13. Grievance contact. BumbleB's Grievance Officer for matters about its own processing is Chinmaya Reddy, reachable at grievance@bumbleb.co.

Annex — United States

1. Scope. This annex applies to Customer Personal Data that is "personal information" or "personal data" under the California Consumer Privacy Act as amended by the California Privacy Rights Act and its regulations (the "CCPA"), or under any other US state privacy law (together, "US Privacy Laws"). Terms such as "business", "service provider", "controller", "processor", "business purpose", "sell", "share", "consumer" and "deidentified" have the meanings given in the applicable US Privacy Law.

2. Roles. Customer is a "business" or "controller", and BumbleB is a "service provider" or "processor", for Customer Personal Data.

3. Specified business purposes. Customer discloses Customer Personal Data to BumbleB, and BumbleB processes it, only for these limited and specified business purposes:

- (a) providing the Service to Customer under the Agreement, including operating the tracking tag on Customer's behalf;
- (b) helping to ensure security and integrity, and detecting and preventing abuse;
- (c) debugging to identify and repair errors, and providing support Customer asks for;
- (d) building or improving the quality of the Service through Usage Data as described in Section 4.4 of this DPA, provided that BumbleB does not use Customer Personal Data to build or modify a profile for use in providing services to another business; and
- (e) complying with the law.

4. Restrictions. BumbleB will not:

- (a) sell or share Customer Personal Data;
- (b) retain, use or disclose Customer Personal Data for any purpose other than the business purposes in paragraph 3, including for any commercial purpose other than those business purposes, or as US Privacy Laws otherwise permit;
- (c) retain, use or disclose Customer Personal Data outside the direct business relationship between Customer and BumbleB; or
- (d) combine Customer Personal Data with personal information it receives from or on behalf of another person, or collects from its own interactions with a consumer, except as US Privacy Laws permit a service provider to do.

5. Usage Data. BumbleB creates Usage Data so that it contains no personal information and keeps it in deidentified form. BumbleB does not sell, share or disclose Usage Data to any third party for that party's own purposes — the only parties that handle it are BumbleB's sub-processors, such as its hosting provider, acting on BumbleB's behalf under contracts that bar them from using it for their own purposes or attempting to re-identify it. BumbleB does not attempt to re-identify Usage Data, and publicly commits to both.

6. Compliance and level of protection. BumbleB will comply with the obligations that apply to it under US Privacy Laws and will provide the same level of privacy protection as US Privacy Laws require of Customer.

7. Consumer requests. BumbleB will assist Customer to respond to consumer requests under US Privacy Laws as set out in Section 9 of this DPA, including requests to know, delete, correct and opt out. Where Customer instructs it, BumbleB will delete the relevant Customer Personal Data and will tell its Sub-processors to do the same.

8. Notice if unable to comply. BumbleB will notify Customer promptly if it determines that it can no longer meet its obligations under US Privacy Laws.

9. Customer's right to stop unauthorised use. Customer may take reasonable and appropriate steps to ensure that BumbleB uses Customer Personal Data consistently with Customer's obligations under US Privacy Laws, including through the audits in Section 13 of this DPA. On notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorised use of Customer Personal Data, and BumbleB will cooperate.

10. Sub-processors. BumbleB will engage Sub-processors under Section 8 of this DPA, will notify Customer of each engagement through the sub-processor list, and will bind each Sub-processor by a written contract that imposes on it the obligations in this annex.

11. Other state laws. For US Privacy Laws other than the CCPA, the confidentiality, deletion and return, information, audit and sub-processor terms in Sections 6, 8, 13 and 14 of this DPA are the terms those laws require a processor contract to contain.

12. Certification. BumbleB certifies that it understands the restrictions in this annex and will comply with them.

Signed for and on behalf of BumbleB Technologies Pvt Ltd (version 2026.3 of the Data Processing Agreement).

Signature */s/ Chinmaya Reddy*

Name Chinmaya Reddy

Title Authorised signatory

Date 9 October 2026