Data Processing Agreement

Pug Cloud · Version 1 · 13 November 2026

This Data Processing Agreement (“DPA”) forms part of the Terms of Service at pug.sh/terms (the “Terms”) between Tshoka Pvt Ltd (“Pug”, “we”) and you, the customer (“Customer”, “you”). It takes effect when you accept the Terms, and applies whenever Pug processes Personal Data on your behalf as part of Pug Cloud. Words defined in the Terms have the same meaning here.

1. Definitions

1.1 “Data Protection Law” means the EU General Data Protection Regulation (Regulation (EU) 2016/679, the “GDPR”), the UK GDPR and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection (“FADP”), and any other data protection law that applies to the processing under this DPA.

1.2 “Customer Data” means the events, properties and profiles you send to Pug Cloud. “Personal Data”, “controller”, “processor”, “data subject”, “personal data breach” and “processing” have the meanings given in the GDPR.

1.3 “Sub-processor” means a third party that Pug engages to process Customer Data.

1.4 “SCCs” means the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914. “UK Addendum” means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

2. Roles and scope

2.1 You are the controller of the Personal Data in Customer Data, or a processor acting for your own controller. Pug is your processor, or your sub-processor.

2.2 Annex I describes the processing: its subject matter, duration, nature and purpose, and the types of Personal Data and data subjects.

2.3 This DPA does not cover data that Pug controls itself, such as your account and billing information. The Privacy Policy at pug.sh/privacy covers that data.

2.4 You are responsible for having a lawful basis for the Customer Data you send, for giving your end users any notice they need and obtaining any consent they must give, including for cookies and similar technologies in your websites and apps, and for the accuracy of Customer Data. You will not send special categories of Personal Data (GDPR Article 9) or data about criminal convictions and offences (Article 10).

3. Your instructions

3.1 Pug processes Customer Data only on your documented instructions. Your instructions are the Terms, this DPA, and your use and configuration of Pug Cloud, including the projects you create, the retention that applies to your plan, and the exports and erasures you request. Any further instruction must be in writing and agreed by both parties.

3.2 Pug will tell you promptly if it believes an instruction infringes Data Protection Law.

3.3 If a law that Pug is subject to requires other processing, Pug will tell you before that processing, unless the law forbids it.

4. Confidentiality

4.1 Pug makes sure that everyone it authorizes to process Customer Data is bound by a duty of confidentiality.

5. Security

5.1 Pug implements the technical and organizational measures in Annex II. Pug may change them, as long as the overall level of protection does not go down.

5.2 You are responsible for the security of your own accounts, API keys, and the systems you connect to Pug Cloud.

6. Sub-processors

6.1 You give Pug general authorization to engage Sub-processors. Annex III lists the current Sub-processors, and the Privacy Policy keeps the list up to date.

6.2 Pug will email your organization's admins at least 30 days before a new Sub-processor starts processing Customer Data. You may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, you may end the Terms for the affected service.

6.3 Pug gives each Sub-processor data protection obligations that protect Customer Data at least as well as this DPA, and remains responsible to you for each Sub-processor's performance.

6.4 A third-party service that you connect to Pug Cloud is not Pug's Sub-processor. This includes a push or email provider you configure with your own credentials, and an AI assistant you connect through Pug's MCP server. Data that Pug sends to such a service goes there on your instructions.

7. Data subject requests

7.1 Pug Cloud lets you answer data subject requests yourself. Through the API you can read a profile and its activity, and erase a profile or a data subject, which deletes their events, the data derived from them, and the profile.

7.2 Where those tools are not enough, Pug will help you as far as reasonably possible. Send the request to hello@pug.sh.

7.3 If a data subject contacts Pug about Customer Data, Pug will refer them to you, and will not answer the request itself unless you instruct it to or the law requires it.

8. Personal data breaches

8.1 Pug will notify you without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Data.

8.2 The notice will describe, as far as Pug knows at the time, what happened, the types and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Pug will send further information as it becomes available.

8.3 Notifying you is not an admission of fault or liability.

9. Assistance

9.1 Taking into account the nature of the processing and the information available to it, Pug will give you reasonable help with data protection impact assessments and with consulting a supervisory authority about Pug Cloud.

10. Return and deletion

10.1 An admin can delete a project and all of its Customer Data in the app at any time.

10.2 When the Terms end, Pug will give you an export of your Customer Data in a machine-readable format (JSON or CSV) if you ask hello@pug.sh within 30 days. Pug deletes Customer Data within 30 days after the Terms end, or after delivering the export you asked for, whichever is later.

10.3 Deleted Customer Data leaves Pug's backups within 30 days, as the backups expire.

10.4 Where the law requires Pug to keep Customer Data, this DPA continues to protect it for as long as Pug keeps it.

11. Audits

11.1 Pug will make available the information needed to show that it complies with this DPA, including by answering reasonable security questionnaires.

11.2 If that information is not enough, you, or an independent auditor bound by confidentiality, may audit Pug on 30 days' written notice. Audits take place no more than once a year, unless a supervisory authority requires one or a personal data breach has occurred, during business hours, at your cost, and without access to other customers' data.

12. International transfers

12.1 Pug Cloud is hosted in Helsinki, Finland, and its backups are stored in the EU. Pug's staff access Customer Data from India, which has no adequacy decision under the GDPR.

12.2 Where the processing involves a transfer of Personal Data from the EEA to Pug, the SCCs form part of this DPA as follows: (a) Module Two (controller to processor) applies where you are a controller, and Module Three (processor to processor) where you are a processor; (b) Clause 7 (docking clause) applies; (c) under Clause 9, Option 2 (general written authorization) applies, with the notice period in section 6.2; (d) the optional wording in Clause 11 does not apply; (e) under Clause 17, Option 1 applies, and the SCCs are governed by the law of Ireland; (f) under Clause 18(b), disputes go to the courts of Ireland; (g) Annexes I, II and III of this DPA complete the Annexes of the SCCs; and (h) the competent supervisory authority under Clause 13 is the one named in Annex I.C.

12.3 Where the UK GDPR applies to the transfer, the UK Addendum forms part of this DPA. Its Table 1 is completed by the parties' details in Annex I, Table 2 by the modules and options in section 12.2, and Table 3 by Annexes I to III. Neither party may end the UK Addendum under its Section 19.

12.4 Where the FADP applies to the transfer, the SCCs apply with these changes: references to the GDPR are read as references to the FADP, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and "Member State" includes Switzerland, so that data subjects in Switzerland can enforce their rights there.

12.5 If the SCCs conflict with this DPA, the SCCs prevail.

13. Liability

13.1 Each party's liability under this DPA is subject to the limits in the Terms, except where Data Protection Law or the SCCs do not allow such a limit.

14. Term, precedence and governing law

14.1 This DPA applies for as long as Pug processes Customer Data for you.

14.2 If this DPA conflicts with the Terms, this DPA prevails for the processing of Personal Data.

14.3 This DPA is governed by the law that governs the Terms, except the SCCs, which are governed as set out in section 12.

Signatures

This DPA applies without a signature. If you want a signed copy, complete the Customer column, sign it, and email it to hello@pug.sh, and Pug will countersign.

	Customer	Tshoka Pvt Ltd
Name		Poluru Praveen Kumar Naidu
Title		Managing Director
Date		
Signature		

Annex I: Description of the processing

A. Parties

	Data exporter	Data importer
Name	The Customer, as identified in its Pug Cloud account	Tshoka Pvt Ltd
Address	The Customer's address, as given at signature	648/A, 4 Flr, Om Chambers, Binnamangala 1st Stage, Bangalore North, Bangalore, Karnataka 560038, India
Contact	The admins of the Customer's Pug Cloud organization	hello@pug.sh
Activities	Use of Pug Cloud	Providing Pug Cloud
Role	Controller (Module Two) or processor (Module Three)	Processor or sub-processor

B. Description of the transfer

Data subjects	People whose activity the Customer sends to Pug Cloud: visitors to and users of the Customer's websites, apps and products, and anyone else the Customer identifies in events or profiles.
Personal Data	Identifiers: anonymous, session, device and user IDs, and the external IDs the Customer assigns. Cookieless visitor IDs, which Pug derives from the IP address and browser details with a key it deletes every day. Event data: event names and times, page URLs, referrers, UTM parameters, and the properties the Customer sends. Profile traits the Customer sends, such as names or email addresses. Device and browser data: browser, operating system, device type, screen size and locale. Approximate location (country, region and city), derived from the IP address when an event arrives; the IP address itself is never stored. Push device tokens, if the Customer uses push campaigns.
Sensitive data	None. The Customer must not send special categories of Personal Data.
Frequency	Continuous, as the Customer's SDKs and API calls send data.
Nature of the processing	Collection, enrichment, storage, aggregation, analysis, display, export and deletion.
Purpose	Providing Pug Cloud to the Customer under the Terms: product analytics, dashboards, user profiles and push campaigns.
Retention	The retention period of the Customer's plan, or until the Customer deletes the data; then as in section 10.
Sub-processors	As listed in Annex III, for the same purpose and duration.

C. Competent supervisory authority

The supervisory authority of the EU Member State where the Customer is established. If the Customer is not established in the EU, the supervisory authority of the Member State where its EU representative is established.

Annex II: Technical and organizational measures

Area	Measures
Hosting	Pug Cloud runs on Hetzner servers in Helsinki, Finland. Databases accept connections only from Pug's private network.
Encryption	Traffic to Pug's websites and API is encrypted with TLS. Backups are encrypted at rest. SSO client secrets and per-organization email provider credentials are stored encrypted.
Staff access	Production access is limited to named Pug staff and uses key-based authentication.
Customer access	Organization roles (admin, member, viewer) are checked on every request, and every query is scoped to the project that owns the data. Passwords are stored as salted hashes. Private API keys, refresh tokens and sign-in links are stored only as hashes.
Data minimization	Raw IP addresses are never stored. Cookieless mode counts visitors under identifiers that change every day, with a key that is deleted every day. Automated traffic is tagged as bots.
Deletion	Data subject erasure deletes the person's events, the data derived from them, and their profile. Deleting a project erases all of its data. A daily job deletes events older than each organization's retention period, a month at a time. Expired tokens are deleted daily.
Backups and availability	Postgres is backed up daily with point-in-time recovery, and ClickHouse nightly. Backups are kept for 30 days in Cloudflare R2, in the EU. Message streams are replicated across three nodes.
Monitoring	Systems are monitored with a self-hosted observability stack in the same region. Server logs are kept for up to 30 days.
Development	The code is open source. Dependencies are updated through automated pull requests and checked for known vulnerabilities.
Abuse protection	Password sign-in and sign-in link requests are protected by Cloudflare Turnstile.
Incidents	Customers are told of a personal data breach within 48 hours (section 8).

Annex III: Sub-processors

Sub-processor	Purpose	Location	Transfer safeguard
Hetzner Online GmbH (Germany)	Hosting of Pug Cloud's servers, databases and monitoring	Helsinki, Finland	Within the EU
Cloudflare, Inc. (United States)	Network edge (TLS, DNS, content delivery, bot checks) and backup storage	Global network; backups in the EU	EU-US Data Privacy Framework and SCCs

Pug also uses providers that handle only account data, not Customer Data, such as email delivery, error monitoring and payments. The Privacy Policy lists them.