Data Processing Addendum – Brave Search API

1. Purpose and scope

(a) The purpose of this Data Processing Addendum (DPA) is to ensure compliance with applicable legal obligations around the processing of personal data. This DPA reflects the Parties' agreement with respect to the processing of personal data by Brave Software, Inc. (hereinafter, "BSI"). Unless otherwise specified in this Addendum, BSI acts as a processor of personal data on behalf of the controller, as specified in Annex I.

(b) Both Parties listed in Annex I have agreed to this DPA in order to ensure compliance with Applicable Data Protection Laws.

(c) This DPA applies to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of this agreement.

(e) This DPA is without prejudice to obligations to which the controller is subject by virtue of other Applicable Data Protection Laws or other legal obligations.

(f) **This DPA does not apply to BSI's processing of Search Query Data made through the search application programming interface ("Brave Search API").** Search Query Data does not relate to an identified or identifiable natural person, individual, or consumer; as such, BSI's processing, storage, and retention of Search Query Data does not fall within the material scope of processing personal data or personal information, as those terms are defined under the Applicable Data Protection Laws.

With respect to Search Query Data collected via the Brave Search API, BSI is not considered a processor, service provider, or third party of personal data or information within the meaning of the Applicable Data Protection Laws.

2. Definitions

(a) The term "Search Query Data" refers to the queries generated by customers directly to one or more Brave Search endpoints via the Brave Search API. Brave Search API endpoints include: web, image, video, and news services, as well as summarization, spellcheck, and suggestions.

(b) For purposes of this agreement, the terms "personal data", "processing", "processor", "controller", "data subject", and "sub-processor", shall have the meanings given to them under the EU GDPR or UK GDPR.

(c) The terms "personal information", "business purpose", "service provider", "business", "consumer", and "third party", as defined under Cal. Civ. Code §1798.140, shall be equivalent and interchangeable with the terms defined in point 2(a) of this section.

(d) The term "Applicable Data Protection Laws" shall refer to the following laws:

- EU General Data Protection Regulation, Regulation (EU) 2016/679;

- UK General Data Protection Regulation, Data Protection Act 2018;
- The California Consumer Privacy Act, as amended by the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and other similar data protection laws that may be relevant.

3. Interpretation

(a) This DPA shall be read and interpreted in the light of the provisions of the Applicable Data Protection Laws.

(b) This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for under the Applicable Data Protection Laws, or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.

5. Description of the processing activities

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

6. Obligations of the parties

6.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by law of which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe on Applicable Data Protection Laws.

6.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

6.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

6.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with this DPA and the Applicable Data Protection Laws.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this DPA.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and the Applicable Data Protection Laws. At the controller's request, the processor shall also permit and reasonably contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice. The controller will be limited to one (1) on-site audit in a calendar year. Any on-site audit, whether done by the controller directly, or through a mandated independent auditor, must be done:

(1) reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the services provided;
(2) with at least four weeks' advance written notice. If an emergency justifies a shorter notice period, the processor will use good faith efforts to accommodate the request; and
(3) during the processor's normal business hours, under reasonable duration and in a manner that does not unreasonably interfere with the processor's day-to-day operations.

Prior to the commencement of any on-site audit, the Parties shall mutually agree to the scope, time, and duration, and reimbursement rate to the processor, for which the controller shall be solely responsible. Processor shall have the right to reasonably adapt the scope of any on-site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other customers' information.

(e) The Parties shall make the information referred to in this Addendum, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7. No sale or sharing of personal information.

(a) The service provider agrees to process data only for the stated business purpose(s) and/or services as described in this DPA. The service provider (and any contracted companies acting on behalf of the service provider) hereby agree, represent, and warrant that it will not:

(1) sell or share personal information a) provided by the business; or b) processed on behalf of the business;
(2) process personal information outside the scope of this relationship (unless required by applicable law);
(3) combine personal information with other personal data or information collected or received from other sources; or
(4) retain, use, or disclose the personal information it receives from the business, or outside the business relationship when collected directly from a consumer, for any other purpose than the business purpose(s) and/or service(s) specified in Annex II of this Addendum, except as otherwise permitted under the Applicable Data Protection Laws.

(b) The service provider certifies that it understands its contractual restrictions as set forth in this clause, and that it shall comply with them.

(c) The service provider shall notify the business if the service provider determines that it can no longer meet its obligations under this Section 6.7.

6.8. Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION:** The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to this DPA and to the Applicable Data Protection Laws.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

6.9. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under laws to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

7. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall reasonably assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 7(b), the processor shall furthermore reasonably assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679 or other Applicable Data Protection Laws.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

8. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and reasonably assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or based on obligations under other applicable laws that the controller is subject, taking into account the nature of processing and the information available to the processor.

8.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall reasonably assist the controller, at the controller's expense:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information pursuant to Applicable Data Protection Laws, which shall at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) complying with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under the Applicable Data Protection and other relevant laws.

9. Non-compliance with this Addendum and termination

(a) In the event that the processor is in breach of its obligations under this DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this DPA or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with this DPA, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with this DPA if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of this DPA or its obligations under the Applicable Data Protection Laws;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or to the Applicable Data Protection Laws.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under this DPA where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name: **[TO BE COMPLETED BY CUSTOMER]**

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

Processor(s):

Name: **Brave Software, Inc.**

Address: **580 Howard St. Unit 402, San Francisco, CA 94105**

Contact person's name, position and contact details: **Peter Davey, Brave DPO, privacy@brave.com**

Signature and accession date:

ANNEX II: DESCRIPTION OF THE PROCESSING FOR BRAVE SEARCH API

Nature of Engagement	Use of the Brave Search API by Customer	
Summary Description of Services and Purposes of Processing	Brave Software Inc. (the Company) will collect and process personal data necessary to provide the Brave Search API service on behalf of the Customer.	
Categories of personal data to be processed	• Full Name • Account ID (assigned by Brave) • Email address • Contact information • Hashed identifier (provided by Stripe) • Other information shared by Account holders with the Company (for billing/support queries)	
Categories of Data Subjects	Account holders	
Processing activities and lawful basis	Creation & management of accounts	Necessary for the performance of a contract. **Data retained after account closure**: Legitimate interests, compliance with legal obligations
	Providing customer support	Performance of a contract with the Account holder.
	Processing payments based on Customer's use of the Brave Search API	Performance of a contract with the Account holder. Legitimate interests.
	Resolving billing enquiries and troubleshooting API usage issues	Performance of a contract with the Account holder. Legitimate interests.
	To prevent abuse of the Search API	Legitimate interests.
	Compliance with the Company's legal obligations	Legal obligation
Data retention	Details on the duration of storage can be found at https://api-dashboard.search.brave.com/app/documentation/general/privacy-policy and in Annex IV.	
Frequency of the transfer	Occasional / ad hoc	
Contact	privacy@brave.com	

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Brave is currently in the process of obtaining full SOC 2 attestation (ETA September 2025). Our Search API specific security practices are available here:
https://api-dashboard.search.brave.com/app/documentation/general/security

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller.

As specified by the contractual agreements and data processing addendums signed with our sub-processors.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

As defined in this agreement.

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name of Subprocessor	Data Storage Location	Processing Activities	Duration of Processing	Onward Transfer Mechanisms	Types of Personal Data Processed
Amazon	United States	Search API queries (both processing and storage); Account access & provisioning	90 days for search query logs; 12 months from when an account is deleted. Option for Zero Data Retention (Enterprise clients), subject to BSI legal obligations.	SCCs	Email address, full name and account ID (assigned by Brave).
Stripe	United States	Payments processing	12 months from when an account is deleted.	EU-US Data Privacy Framework / UK-US & CH-US DPFs	A hashed identifier received from Stripe, that links to the account within Stripe system.
Alphabet / Google	United States	Customer support (emails sent to support@/privacy@brave.com)	Maximum six years.	SCCs	Email address, name, contact information, other information provided by user.
Slack	United States	Internal communications	Slack will process personal data for the duration of the agreement, unless otherwise agreed upon in writing.	Salesforce Processor BCRs / SCCs (UK, Switzerland)	First and last name, contact information, ID data, other data as required for ticket resolution.
Oracle NetSuite	United States	Invoicing	Returned after contract termination.	Oracle Processor BCRs	Account information, client contact information, billing details.
Asana	United States	Inbound inquiries for custom agreements	Asana will retain information for the period necessary to fulfill the purposes until termination of the agreement.	EU-US Data Privacy Framework / UK-US & CH-US DPFs	Customer prospect information such as name, email address, contact information.

Details about subprocessors will be updated as necessary and provided at:
https://api-dashboard.search.brave.com/app/documentation/general/privacy-policy