

Babel Street, Inc.
Data Processing Addendum

Last Updated: 02.26.25

This Data Processing Addendum (“**Addendum**”) is an addendum to the Babel Street End User Subscription Terms (“**Agreement**”) governing Customer’s use of the Babel Street Services. This Addendum applies to the extent that Babel Street acts as a Processor to the Customer as a Controller, in relation to the Processing by Babel Street of Personal Data. All capitalized terms used herein but not defined herein shall have the meaning given to such terms in the Agreement.

1. Key definitions.

The following terms shall have the following meanings:

“**Affiliate**” means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with a Party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

“**Applicable Data Protection Law**” means any applicable legislative or regulatory regime enacted by a recognized government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons or households consisting of natural persons, including without limitation the General Data Protection Regulation 2016/679 (“GDPR”) and supplementing data protection law of the European Union Member States; the United Kingdom’s Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018 (“UK GDPR”); the Swiss Federal Data Protection Act (“Swiss DPA”); Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”) S.C. 2000, ch. 5, and any provincial legislation deemed substantially similar to PIPEDA under the procedures set forth therein; and any applicable laws of any United States jurisdiction, including without limitation the California Consumer Privacy Act of 2018 and California Privacy Rights Act (together, the “CPRA”), the Colorado Privacy Act, the Virginia Consumer Data Protection Act, and any other such applicable law that comes into effect during the term of the Agreement.

“**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.

“**Data Subject**”, “**Data Protection Impact Assessment**”, “**Personal Data Breach**”, “**Process/Processed/Processing**”, “**Processor**”, and “**Supervisory Authority**” have the meaning set out in the GDPR, and the terms “business,” “service provider,” “sell” and “share” shall have the same meaning as set forth in Applicable Data Protection Laws, and their cognate terms shall be construed accordingly.

“**Personal Data**” means any structured set of information relating to an identified or identifiable natural person (‘data subject’) which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis and which are obtained by or made available to Babel Street in connection with the Services.

“**Processed Personal Data**” means the Personal Data to be processed in connection with the Parties’ obligations under the Agreement and this Addendum.

“**Services**” means the Babel Street Application and/or Services described in the Agreement or an Order Form to which Customer has subscribed.

“Subprocessors” means third party organizations that Babel Street engages for the Processing of the Personal Data and which do not act under Babel Street’s direct authority.

2. Compliance with the Customer’s Instructions

Babel Street shall be a Processor Processing Personal Data on behalf of the Customer, acting as a Controller, and this Addendum shall apply accordingly. Babel Street may only process Personal Data in connection with its provision of the Service(s) to Customer pursuant to the Agreement and as set out in Attachment A, or as otherwise in accordance with the documented instructions of Customer (which may be provided to Babel Street from time to time, including for example by way of letter of instruction or through the Customer’s use of Babel Street settings, controls or other user preference functionality within the Service(s)), or required by Applicable Data Protection Law. The subject-matter, duration, nature and purpose of the Processing, types of Personal Data and categories of individuals will be the same as for the relevant Term of Customer’s access to the Service(s) to which the Processing relates. Customer represents and warrants that: (i) its use of the Services and the documented instructions provided do not contravene Applicable Data Protection Law; (ii) it has complied and continues to comply with Applicable Data Protection Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and/or otherwise has the right to disclose Personal Data to Babel Street and enable the Processing set out in this Addendum and as contemplated by the Agreement; (iii) it has assessed the requirements under Applicable Data Protection Law as they apply to Customer with regard to Personal Data and finds that the security measures referenced are adequate to meet those requirements; and (iv) it will ensure compliance with and shall not in any way alter or diminish such security measures to the extent applicable to Customer through its use of the Service(s). Where Customer is a Processor of the Personal Data covered by this Addendum, Babel Street shall be a Subprocessor of the Personal Data and this Addendum shall apply accordingly. Any Processing unrelated to the provision of the Service(s) set forth in Attachment A I will require additional consent and approval of the Parties. For the avoidance of doubt, Babel Street shall not engage in the sale of Customer’s Personal Data within the meaning of the CCPA.

3. Security

Customer acknowledges that the Service(s) are not designed with security and access management for processing the following categories of information: (a) "Protected Health Information" or "PHI" as that term is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and its implementing regulations at 45 CFR §160.103; (b) “Cardholder Data” or “Sensitive Authentication data”, as such terms are defined in the Payment Card Industry Data Security Standard (PCI DSS). Notwithstanding the foregoing, Babel Street will implement appropriate technical and organizational measures for the Service(s) that are designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, disclosure or access, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, including, but not limited to, the measures set forth in Attachment B to this Addendum. In such event, Babel Street shall notify Customer without undue delay and in accordance with Applicable Data Protection Law. Such security procedures and practices include an information security program consistent with the NIST 800-171 Standards and ISO 27001 requirements.

4. Audits

Upon Customer's request, Babel Street shall, no more than once per calendar year, make available for Customer's review, copies of certifications or reports demonstrating Babel Street's compliance with prevailing data security standards applicable to the Processing of Customer's Personal Data. If the Customer and Babel Street have entered into SCCs (defined below), the Customer's right to audit Babel Street's activities under the SCCs shall be interpreted in line with this Addendum, so as to be satisfied by the audit rights provided to the Customer.

5. Assistance

Babel Street shall, taking into account the nature of the Processing and the information available to Babel Street, assist Customer in ensuring compliance with its obligations under Applicable Data Protection Law to conduct a data protection impact assessment and, with prior notice, to assist with consultations with the Supervisory Authority, where required. In the event of a confirmed Personal Data Breach, Babel Street shall provide notification to Customer consistent with the General Data Protection Regulation, Regulation (EU) 2016/679, or other applicable law, and take such steps as Babel Street in its sole discretion deems necessary and reasonable to remediate such Breach. In the event of such a Personal Data Breach, Babel Street shall, taking into account the nature of the Processing and the information available to Babel Street, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (i) the relevant Supervisory Authority and/or (ii) Data Subjects affected by such Personal Data Breach. These obligations shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer, except where required by Applicable Data Protection Law. Babel Street's obligation to report or respond to a Personal Data Breach under this section will not be construed as an acknowledgement by Babel Street of any fault or liability with respect to the Personal Data Breach.

6. Individuals

If Babel Street receives requests directly from individuals in relation to the Processing of their Personal Data used by Customer through the Service(s), Babel Street will notify Customer of the request, without responding to it, unless Babel Street has been authorized to respond, or is prohibited from doing so under applicable law. Customer is solely responsible for providing any necessary notices to, and obtaining any necessary consent from, individuals with respect to the Processing of Personal Data pursuant to the Agreement.

7. Subprocessors

Customer agrees that Babel Street may use Subprocessors to assist Babel Street in Processing Personal Data for the performance of the Agreement, provided that:

- (i) Babel Street imposes no less stringent duties on such Subprocessors regarding security and confidentiality of Personal Data as those set out in this Addendum.
- (ii) Babel Street remains responsible to Customer for the performance of the relevant Service(s) by the Subprocessor, and
- (iii) Babel Street maintains a list of such Subprocessors and will provide Customer with reasonable notice of any addition of Subprocessors. Customer may within five (5) days of receiving the notice, object to the involvement of such new Subprocessor in the delivery of the Service(s) through providing notice of objective justifiable grounds related to the ability of such Subprocessor to protect the Personal Data or comply with data protection requirements applicable to Subprocessor. In the event that the objection is not unreasonable, the parties will work together in good faith to find a solution to address such objection including but not limited to reviewing additional documentation supporting the Subprocessors' compliance or trying to

make the Service(s) available without the involvement of such Subprocessor. If the foregoing is not commercially feasible, Babel Street may terminate Customer's access to the Service(s) in accordance with the Agreement.

8. Transfers

Customer acknowledges and agrees that Babel Street may transfer to and Process Personal Data in the United States and anywhere else in the world where Babel Street, its Affiliates, or its Subprocessors maintain Processing operations. Babel Street shall ensure that such transfers are made in compliance with Applicable Data Protection Laws and this Addendum.

EEA. The Parties acknowledge and agree that each Party may Process Personal Data and/or permit Personal Data to be Processed in accordance with this Addendum in a territory outside the European Economic Area ("EEA") or Switzerland. Therefore, for the purposes of compliance with Applicable Data Protection Laws relating to cross-border transfers of Personal Data, the Parties have executed the Standard Contractual Clauses published by the European Commission ("SCCs") which are incorporated herein by reference. If required, each Party will ensure that any of its subprocessors also comply with the applicable module of the Standard Contractual Clauses.

Any transfer of Personal Data from member states of the European Union, the EEA (Iceland, Liechtenstein, Norway), and/or Switzerland to any third country that the European Commission has decided does not ensure an adequate level of protection for Personal Data ("Third Country") shall be made in accordance with the SCCs, in connection with which the Parties agree the following:

In relation to Personal Data that is subject to GDPR and Processed in accordance with this Addendum, the SCCs shall apply, completed as follows: Module Two (Controller to Processor transfers) will apply; in Clause 7, the optional docking clause will apply; in Clause 9, the general authorization will apply; in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply and the SCCs will be governed by the law of the Netherlands; in Clause 18(b), disputes will be resolved before the courts of the Netherlands; Annex I of the SCCs shall be deemed completed with the information set out in Attachment A to this Addendum; and Annex II of the SCCs shall be deemed completed with the information set out in Attachment B to this Addendum.

In relation to Personal Data that is subject to the Swiss DPA, the SCCs will apply in accordance with the terms set forth above, with the following modifications: any references in the SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDIPC and competent courts in Switzerland, unless the SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA, in which event the Swiss Standard Contractual Clauses shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss Standard Contractual Clauses shall be populated using the information contained in Attachment A & B to this Addendum (as applicable).

With respect to transfers of personal data originating from the United Kingdom, the Parties acknowledge and agree that the SCCs as modified by this Section shall be read and

interpreted in light of the provisions of UK Data Protection Laws, and so that this Section provides the appropriate safeguards as required by Article 46 of the UK GDPR:

The 'Start Date', 'Parties', and "Key Contact" shall be as listed in Attachment A of this DPA; Clause 6 is replaced with: "The details of the transfers and in particular the categories of personal data that are transferred and the purposes for which they are transferred are those specified in Annex I where UK Data Protection Laws apply to the data exporter's processing when making that transfer"; References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of the UK Data Protection Laws; references to Regulation (EU) 2018/1725 are removed; references to the "Union", "EU" and "EU Member State" are all replaced with the "UK"; Clause 13(a) and Annex I.C are not used; The "competent supervisory authority" is the Information Commissioner's Office (ICO) of the United Kingdom; Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales"; Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the UK GDPR, in which event the UK SCCs shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the UK SCCs shall be populated using the information contained in Attachment A & B to this Addendum (as applicable). Either Party may end the UK Addendum as set out in Section 19 of the UK Addendum to the SCCs, where reasonable and subject to other applicable terms of the Agreement. The Alternative Part 2 Mandatory Clauses shall apply, as follows: Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Babel Street may adopt a replacement data export mechanism (including any new version of or successor to the SCCs or alternative mechanisms adopted pursuant to Applicable Data Protection Laws) ("Alternative Transfer Mechanism"). So long as the Alternative Transfer Mechanism complies with Applicable Data Protection Laws and extends to the territories to which the Personal Data is transferred, Customer agrees to execute any documents and take any other reasonably necessary actions to give legal effect to such Alternative Transfer Mechanism.

It is not the intention of either Party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this Addendum) the SCCs shall prevail to the extent of such conflict.

9. Return and Deletion of Personal Data

Upon termination or expiration of the Agreement, Babel Street will make available to Customer Personal Data maintained by Babel Street for thirty (30) days to allow Customer to retrieve, where reasonably technically feasible and permitted by the Agreement, Personal Data in a commonly used format set out by Babel Street. After such period, Babel Street will destroy or otherwise render inaccessible, at its discretion, such Personal Data from the production environment of the Service(s), except as may be required by law or applicable third-party terms of use. Actions set out in this section are at Customer's sole cost.

10. Changes

Babel Street may make changes to this Addendum from time to time as necessary to reflect changes in its business or legal and regulatory requirements. Babel Street will provide thirty (30) days' notice of any such changes to Customer, at which time, Customer may accept the changes, or terminate the Agreement.

11. General

All terms and conditions of the Agreement shall remain unchanged and in full force and effect. In the event of any conflict or inconsistency between the terms of this Addendum and the Agreement, the terms of this Addendum will control. Any alteration or modification of this Addendum is not valid unless made in writing and executed by duly authorized personnel of both parties. Invalidation of one or more of the provisions under this Addendum will not affect the remaining provisions. Invalid provisions will be replaced, to the extent possible, by such valid provisions which achieve essentially the same objectives. In the event of a change in Applicable Data Protection Law or a determination or order by a Supervisory Authority or competent court affecting this Addendum or the lawfulness of any Processing under this Addendum, Babel Street may (in its sole discretion) make any amendments to this Addendum as are reasonably necessary to ensure continued compliance with Applicable Data Protection Law and/or the Customer's Processing instructions herein.

ATTACHMENT A

A. LIST OF PARTIES

Data processor(s): *Babel Street, Inc.*

Address: *1900 Reston Metro Plaza, #950, Reston, Virginia 20190 USA*

Email: *Privacy@babelstreet.com*

Phone: *+1 (703) 956-3572*

Activities relevant to the data transferred under these Clauses: *Performance of Services under the Agreement*

Data controller(s): *Customer, as defined in the Agreement*

Name: *Customer, as defined in the Agreement*

Activities relevant to the data transferred under these Clauses: *Performance of and/or receipt of Services under the Agreement*

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data is transferred:

- *Search targets of the Babel Street Service(s)*

Categories of personal data transferred:

- *Name and contact details (e.g., location/address, email address, phone number, etc.), citizenship status, marriage status, government ID information, employment history, birth date, educational history, job title(s), criminal background, and/or location data*

Sensitive data transferred (if applicable):

- *May include personal data revealing racial or ethnic origin, political opinions, philosophical or religious beliefs, criminal background, and/or location data*

The frequency of the transfer:

- *The publicly available content will be made available through API connections or file transfers.*
- *Continuous in performance of Service(s) under the Agreement.*

Nature of the processing:

- *Return of publicly available information based on search terms input by Data controller into the Babel Street Service(s).*

Purpose(s) of the data transfer and further processing:

- *The Personal Data will be Processed in the performance of Service(s) under the Agreement.*

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

- *Data will be retained first for as long as specified in the applicable Agreement terms between the parties. Second, data will be retained in compliance with local laws and regulations.*

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

- *The Personal Data transferred may be disclosed only to the following recipients or categories of recipients: Those Subprocessors required by the Parties to allow them to meet their contractual and legal obligations under the Agreement.*

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent EU supervisory authority/ies in accordance with SCC Clause 13:
the Netherlands

ATTACHMENT B

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

EXPLANATORY NOTE:

Below is a description of the technical and organizational measures implemented by Babel Street to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Governance

During the term of this Agreement, Babel Street will maintain compliance with the standards set forth in NIST 800-171 and ISO 27001. This helps drive strategic and operational initiatives to continue to improve our Security Program's maturity. These initiatives include policies, security controls and demonstration of compliance with our regulatory drivers.

Authorization and confidentiality

Access Control Policy

Access controls are established at sites, systems, system documentation, applications, databases, directories, and files (information assets), using automated systems to enforce a role-based access control model, such that users only have access to the information assets necessary to perform their job function. Privileges are set using the principle of least privilege. The default posture will be to deny all access thereby requiring all access that is granted to be granted based on an approved role or access request. Roles are assigned based on user department, team, and job function.

Authentication and Identity Management Policy

All access to information resources shall use an approved method of identification and authentication. All third-party service provider access to the Babel Street network and information systems must adhere to the same access restrictions as internal users.

Access rights shall be established, documented, and periodically reviewed based on business needs and external requirements. Access controls should consider:

- Security requirements given business needs, known threats, and vulnerabilities.
- Relevant legislative and regulatory requirements.
- Contractual obligations and service level agreements.
- Consistency across Babel Street's systems and networks.

Access control considerations include:

- The use of clearly stated rules and rights based on user profiles.
- Consistent management of access rights across information resources using an appropriate mix of logical (technical) and physical access controls.
- Segregation of access control roles including access request by the appropriate department, access authorization by the data owner, and access administration by the network administrator.
- Requirements for the formal authorization and timely removal of access rights.

Personnel

Personnel Security Policy

Information security responsibilities are to be followed by all staff who have access to Babel Street's information resources. All staff must acknowledge that they have read and understood Babel Street's Security Policies. In addition, all staff shall receive annual security-related training. All staff must also sign a Babel Street Non-Disclosure Agreement prior to beginning work for Babel Street.

Code of Conduct

Employees, officers and directors must maintain the confidentiality of confidential information entrusted to them, including our suppliers and customers, except when disclosure is authorized by a supervisor or legally mandated. Unauthorized disclosure of any confidential information is prohibited. Additionally, employees should take appropriate precautions to ensure that confidential or sensitive business information, whether it is proprietary to the company or another company, is not communicated except to employees who have a need to know such information to perform their responsibilities.

Physical security of the operating environment

Security tools and procedures

As part of its core offering, Babel Street leverages Amazon Web Services to deliver its SaaS solution. Before reaching customer instances, network traffic passes through multiple layers of network protections. These include DDOS protection, isolated VLANs, and firewalls. Production environments are segmented from QA and other non-production environments.

In addition to its core infrastructure as defined above, Babel Street maintains its standard approach to secure practices. This is updated annually and includes its coverage of hardware, software, network monitoring protocol and procedure.

Monitoring and logging

Intrusion Detection and/or Prevention Systems must be deployed on all Production systems. These solutions shall be configured to alert personnel to potential information security events. Alerts and security events shall be reported and responded to. These solutions shall also be maintained with updated patches and signatures on a regular basis – at least weekly when available.