Data Processing Agreement

Effective Date: As stated above in the Agreement

This Data Processing Agreement and the Annexes (in the following collectively referred to as "DPA") reflects agreement with respect to the Processing of Personal Data between Toloka (the "Processor") and Customer (the "Controller"), in connection with the Services Toloka provides under Toloka Terms of Use.
This DPA is supplemental to, and forms an integral part of, the Toloka Terms of Use (the "Agreement") concluded by the parties. Parties may update the terms of this DPA if required by law, changed circumstances, jurisprudence or other developments. Parties will inform of these changes via email and/or other ways. Parties agree as follows:

ROLES

When Processing Personal Data in accordance with Customer's instructions, the parties acknowledge and agree that Customer is acting as the Controller and Toloka is the Processor under the Agreement.

DEFINITIONS

2.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
2.2. "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq., as may be amended from time to time, including the California Privacy Rights Act.
2.3. The terms, "Controller", "Member State", "Processor", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR. The terms "Business", "Business Purpose", "Consumer" and "Service Provider" shall have the same meaning as in the CCPA. For the purpose of clarity, within this DPA "Controller" shall also mean "Business", and "Processor" shall also mean "Service Provider", to the extent that the CCPA applies.
2.5. "Data Protection Laws" means all applicable and binding privacy and data protection laws and regulations, including, but not limited to, General Data Protection Regulation (GDPR), Federal Act on Data Protection 2020 (FADP), UK GDPR, Serbian Law on Protection of Personal Data 2018, and other laws, as applicable to the Processing of Personal Data hereunder and in effect at the time of Processor's performance hereunder.
2.6. "Data Subject" means the identified or identifiable person to whom the Personal Data relates.
2.7. "FADP" means the Swiss Federal Act on Data Protection of 19 June 1992, and as of 25 September 2020, the "Revised FADP".
2.8. "GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2.9. "Personal Data" or "Personal Information" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer, which is processed by Toloka on behalf of Customer, under this DPA and the Agreement
2.10. "Services" means the services provided to Customer by Toloka in accordance with the Agreement.
2.11. "Security Documentation" means the Security Documentation applicable to the Services purchased by Customer as made available to Customer by Toloka.
2.12. "Standard Contractual Clauses" mean the standard contractual clauses set out in the Annex of European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, in the FDPIC's decision "The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts" of 27 August 2021 and the UK's international data transfer addendum to the European Commission's standard contractual clauses for international data transfers of 21 March 2022.
2.13. "Sub-processor" means any third party that Processes Personal Data under the instruction or supervision of Toloka.
2.14. "UK GDPR" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).
2.15. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Processor and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

CONTROLLER'S OBLIGATIONS

3.1. Compliance with Laws. Controller is responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions issued to the Processor. In particular but non exclusively, the Controller acknowledges and agrees that it is solely responsible for: (i) the accuracy, quality, and legality of the data provided to Processor; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations, (particularly for use by Customer for marketing purposes); (iii) ensuring it may legally transfer or provide access to, the Personal Data which Processor will be processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that the instructions imparted to Processor comply with applicable laws, including Data Protection Laws. The Controller will moreover inform the Processor without undue delay if Controller it is not able to comply with its responsibilities under section or applicable Data Protection Laws.
3.2. Security Measures. Controller is responsible for a secure use of the Services offered by Processor, and it is responsible for independently determining whether the data security provided adequately meets the obligations under applicable Data Protection Laws.

PROCESSOR'S OBLIGATIONS

4.1. Compliance with Applicable Law and Instructions. Processor shall comply with all applicable Data Protection Laws in the Processing of Customer Personal Data;
4.2. Instructions. If the Processor believes that Controller's Instruction infringes Applicable Data Protection Laws (where applicable), it will inform Controller without delay. Nevertheless, such notification will not constitute a general obligation on the part of the Data Processor to monitor or interpret the laws applicable to the Controller, and such notification will not constitute legal advice to the Controller.
4.3. Conflict of Laws. Processor will immediately notify the Controller when it becomes aware of the impossibility to process Personal Data in accordance with the instructions received by Controller due to a legal requirement under any applicable law, Processor will. In this case, if necessary, the Processor will cease all processing activities, (other than merely storing and maintaining the security of the affected Personal Data) until new lawful instructions are received from the Controller. If such a situation occurs, Processor will not be liable to Controller for any non-compliance until Controller issues new lawful Instructions.
4.4. Security. Processor implements and duly maintains appropriate technical and organizational measures to protect Personal Data, as described under Annex II to this DPA ("Security Measures"). Processor may modify or update the Security Measures at its own discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.
4.5. Confidentiality. Processor ensures that all employees authorized to process Personal Data on our behalf are subject to appropriate confidentiality obligations with respect to that Personal Data.
4.6. (Personal) Data Breaches. Processor will notify the Controller without undue delay after it becomes aware of any Personal Data Breach and will provide the necessary information relating to the Personal Data Breach as requested by the Controller. At Controller's request, the Processor will promptly provide reasonable assistance as necessary to enable the Controller to notify relevant Personal Data Breaches to the competent authorities and/or to the affected Data Subjects, if required under Data Protection Laws.
4.7. Deletion or Return of Personal Data. Processor will delete or return, at the free choice of the Controller, all Personal Data processed on behalf of the Controller, (including copies thereof), on termination or expiration of the Services provided under the Agreement within timeframes specified by Controller. As a sole exception Processor will retain (part of) the Personal Data in case and within the limit such is required by applicable law.
4.8. Data Protection Impact Assessments and Supervisory Authorities. To the extent that the required information is reasonably available to us, and Controller has no otherwise access to the required information, Processor will provide reasonable assistance with any data protection impact assessments, and prior consultations with supervisory authorities (for example, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), Federal Data Protection and Information Commissioner (FDPIC) and the UK Information Commissioner's Office (ICO)) or other competent data privacy authorities to the extent required by Applicable Data Protection Laws.

DATA SUBJECT REQUESTS

5.1. Considering the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
5.2 When a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is received directly by the Processor, the Processor will promptly inform the Controller and ask the Data Subject to submit their request to the Controller. The Controller will be solely responsible for addressing and responding to any such Data Subject Requests.

SUB-PROCESSORS

6.1. Engaging. Controller allows engaging Sub-Processors (including Tolokers). When engaging Sub-Processors, Processor will impose data protection terms on these Sub-Processors providing at least the equivalent level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. Processor remains responsible for Sub-Processor's compliance with the obligations of this DPA.
6.2. List. Controller hereby agrees that Processor may engage Sub-Processors to Process Personal Data on its behalf, a list of the current Sub-Processor is enclosed as Annex IV of this DPA.
6.3. Changes. If Processor adds or changes one or more Sub-Processor(s), it will notify Controller at least 30 days prior to any such change and provide Controller the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 15 days. In case Controller notifies Processor of such an objection, both parties will discuss the concerns in good faith, aiming at achieving a reasonable solution. If no such solution can be reached, Processor will either not appoint the intended new Sub-Processor or allow Controller to terminate the Service in accordance with the termination provisions of the Service Agreement without prejudice to any fees incurred by Controller prior to suspension or termination, but without liability to either party.
6.4. Engaging of Users. List of Users that were engaged to complete a Task of Controller can be seen using the interface of the Toloka Platform in the form of hashes assigned to the User(s). Controller may restrict the region of Users for performance of its Tasks via the tools of Toloka Platform.
6.5. Standard Contractual Clauses. For compliance with Article 46 GDPR, Article 46 UK GDPR and Article 17 FADP Processor ensures to conclude Standard Contractual Clauses (SCC) as applicable. Standard Contractual Clauses must be incorporated in accordance with Commission Implementing Decision (EU) 2021/914 of 4 June 2021. The Customer and Processor agree that the following options shall be used in the SCCs concluded with any Sub-Processors:
i. in Clause 11(a) Option shall apply;
ii. in Clause 17 Option 2 shall apply.
6.6. In relation to Personal Data that is subject to the GDPR:
i. Processor is the "data exporter" and Sub-Processor is the "data importer";
ii. the Module Three terms apply.
6.7. In relation to Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with the following modifications:
i. the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement.
6.8. In relation to Personal Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with the following modifications
i. references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA.
6.9. Any dispute arising from SCC shall be resolved by the courts:
For the EU: of the Netherlands;
For Swiss: of Switzerland;
For the UK: Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings 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.

REPORTS, SECURITY AND AUDITS

7.1. Controls for the Protection of Personal Data. Processor represents and warrants that it has implemented and will maintain all appropriate technical and organizational measures for protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation). Upon the Controller's request, Processor shall assist Controller, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR and under the Security Regulations.
7.2. Records of Processing. Processor will duly maintain records of its Processing activities performed on behalf of Controller.
7.3. Audits and Inspections. Upon prior written request, and subject to confidentiality undertakings by Controller, Processor shall make available to Controller (or Controller's independent third-party auditor subject to their confidentiality undertakings) all reasonable information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them. If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 6.5 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses. In the event of an audit or inspections as set forth above, Controller shall take reasonable steps to avoid causing (or, if it cannot avoid, minimize) any disruption to Processor's operations while conducting such audit or inspection.
7.4. Reports. Upon written request made by Controller and limitedly to once a year, except if substantial elements arise indicating the non-compliance of Processor with the requirements of Applicable law and of this DPA, Processor will provide Controller with a report demonstrating Processor's compliance with its obligations under this DPA and Applicable Law.

GENERAL PROVISIONS

8.1 Severability. If any individual provisions of this DPA is invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.
8.2. Limitation of Liability. Each Party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other DPAs between the parties) and the Standard Contractual Clauses, where applicable, will be subject to the limitations and exclusions of liability set out in the Agreement.
8.3 Governing Law. This DPA will be governed by and construed in accordance with laws specified in clause 10.1. of the Agreement.
8.4 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, shall be resolved in accordance with clause 10.2. of the Agreement.

ANNEX I – LIST OF THE PARTIES

List of parties

Controller (Customer):
Legal entity, or sole trader, or individual who accepted Toloka Terms of Use or signed the Master Service Agreement for the provision of Toloka Services (each referred as "Agreement").

Processor (Toloka):
Toloka AI AG
Werftestrasse 4, 6005 Luzern, Switzerland
Contact person's name, position and contact details: privacy@toloka.ai.

ANNEX II – DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed
Natural persons whose personal data are contained in Customer's dataset and/or are required to perform Tasks.

Categories of personal data processed
Any personal data contained in Customer's dataset and/or required to perform Tasks.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Sensitive personal data contained in Customer's dataset and/or required to perform Tasks. Strict purpose limitation and access restrictions are employed.

Nature of the processing
The processor provides the controller with Services specified in Toloka Terms of Use or Master Service Agreement for the provision of Toloka Services entered by the Parties. The processor performs on behalf of the controller operations on personal data required to provide Toloka Services: Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure, and destruction.

Purpose(s) for which the personal data is processed on behalf of the controller
1. Providing the Services to Controller;
2. Performing the Agreement, and this DPA;
3. Acting upon Controller's written instructions in accordance with the Agreement;
4. Complying with applicable laws and regulations.

Duration of the processing
The processor will retain Personal data for the term of the Agreement plus the period from expiry of the term of the Agreement until deletion of Personal data by the processor in accordance with this Data Processing Agreement.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing
In relation to transfers to sub-processors, the subject matter, and nature of the processing is set forth in Annex IV of the DPA. The duration of the processing by sub-processors is the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

ANNEX III – SECURITY MEASURES

Technical and organisational measures including technical and organizational measures to ensure the security of the data
Description of the technical and organizational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

- For the secure storing and processing of personal data, we use the Microsoft Azure platform, which provides the highest level of data protection in the industry. The platform is certified according to the basic information security standards: CSA, SOC2, ISO 27001, and etc.
- Information security management system has been implemented and certified with SOC2 Type 1, ISO 27001 and ISO 27701;
- TLS is used to protect data during transmission. TLSv1.3 is supported;
- Centralized authentication system implemented in Azure and used to ensure secure user management. Access control process has been implemented;
- All data bases are encrypted at rest;
- Backups are performed daily. All backups are encrypted;
- The processor has developed and adopted a number of policies, including but not limited to:
  - Information Security Policy
  - Sensitive User Data Usage Policy
  - Incident Management Policy
  - Malware Protection Policy
  - Regulations for Access Control

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller:
For transfers to sub-processors that are necessary to ensure technical measures that data subjects are afforded a level of protection that is essentially equivalent to that are implemented by the processor(s).
Description of the specific technical and organizational measures to be taken by the processor to be able to provide assistance to the controller:
Technical and organizational measures to be taken by the processor to be able to provide assistance to the controller are afforded a level of protection that is essentially equivalent to that are implemented by the processor(s).

ANNEX IV – SUB-PROCESSORS

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

1

Name:	Microsoft Azure (Microsoft Corporation)
Address:	Redmond, One Microsoft Way, United States
Hosting location:	USA or East Europe (depends on controller's instructions). East Europe is a default storage location
Contact person's name, position and contact details:	online web-form
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Cloud storage

2

Name:	Databricks, Inc.
Address:	160 Spear Street, 13th Floor San Francisco, CA 94105
Hosting location:	EU
Contact person's name, position and contact details:	Scott Starbird, General Counsel, Public Affairs and Strategic Partnerships, dpa@databricks.com
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Product data analytics

3

Name:	Sentry.io (Functional Software, Inc.)
Address:	45 Fremont Street, 8th Floor, San Francisco, CA 94105
Hosting location:	USA
Contact person's name, position and contact details:	Virginia Badenhope, General Counsel, legal@sentry.io
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Error monitoring

4

Name:	Zendesk (Zendesk, Inc.)
Address:	989 Market Street San Francisco, CA 94103, United States
Hosting location:	USA
Contact person's name, position and contact details:	euprivacy@zendesk.com or privacy@zendesk.com
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Support service (ticketing system)

5

Name:	Toloka d.o.o. Beograd
Address:	Starine Novaka 23, Sprat 4, Belgrade (Palilula). 11000, Belgrade, Serbia
Hosting location:	Serbia
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Support and Maintenance of Toloka Services

6

Name:	Tolokers (as defined in the Agreement) who will be engaged to perform Controller's tasks via Toloka Platform. List of Tolokers that were engaged to complete a Task of the controller can be seen using the interface of the Toloka Platform in the form of hashes assigned to the Toloker. The controller may restrict the region of Tolokers (Users) for performance of its tasks via the tools of Toloka Platform.

7

Name:	OpenAI, L.L.C.
Address:	3180 18th St, San Francisco, CA 94110
Hosting location:	USA
Contact person's name, position and contact details:	privacy@openai.com
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	LLM Services Provider

8

Name:	Tableau Cloud (Salesforce, Inc)
Address:	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California, 94105, USA
Hosting location:	USA
Contact person's name, position and contact details:	privacy@salesforce.com
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Analytics