Data Processing Agreement

Effective Date: As stated above in the Agreement

Last Updated: February 27, 2025

This Data Processing Agreement, including its Annexes (collectively referred to as the "DPA"), governs the Processing of personal Data between Toloka (the "Processor") and Customer (the "Controller"), in connection with the Services provided by Toloka under the Toloka Terms of Use.

This DPA is supplemental to and forms an integral part of the Toloka Terms of Use (the "Agreement") entered into by the parties.

The parties may update the terms of this DPA as required by law, due to changing circumstances, jurisprudence, or other developments. The parties will inform of such changes via email and/or other appropriate means.

The parties agree as follows:

ROLES

When Processing Personal Data in accordance with the Customer's instructions, the parties acknowledge and agree that the Customer acts as the Controller and Toloka as 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. For the purposes of this definition, "control" 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 defined in the CCPA. For clarity, within this DPA "Controller" shall also mean "Business", and "Processor" shall also mean "Service Provider", to the extent the CCPA applies.

2.4. "Data Protection Laws" means all applicable and binding privacy and data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR), the Swiss Federal Act on Data Protection 2020 (FADP), the UK GDPR, the Serbian Law on Protection of Personal Data 2018, and any other laws applicable to the Processing of Personal Data under this DPA, as in effect at the time of Processor's performance.

2.5. "Data Subject" means an identified or identifiable person to whom the Personal Data relates.

2.6. "FADP" means the Swiss Federal Act on Data Protection of 19 June 1992, and as of 25 September 2020, the "Revised FADP".

2.7. "GDPR" means 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).

2.8. "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 the Customer under this DPA and the Agreement.

2.9. "Services" means the services provided to the Customer(s) by Toloka in accordance with the Agreement.

2.10. "Standard Contractual Clauses" means:

i. the standard contractual clauses set out in the Annex of European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

ii. 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 as of 27 August 2021; and

iii. the UK's international data transfer addendum to the European Commission's standard contractual clauses for international data transfers of 21 March 2022.

2.11. "Sub-processor" means any third party that Processes Personal Data under the instruction or supervision of Toloka.

2.12. "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).

2.13. "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 is transmitted, stored or otherwise Processed by the Processor and/or its Sub-Processors in connection with the provision of the Subscription Services. A Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data. Such activities include, but are not limited to, 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. The Controller is responsible for ensuring compliance with all applicable Data Protection Laws concerning its Processing of Personal Data and the instructions issued to the Processor. In particular, but not 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 the Customer for marketing purposes);

(iii) ensuring that it may legally transfer or provide access to the Personal Data that the Processor will process in accordance with the terms of the Agreement (including this DPA);

(iv) ensuring that the instructions provided to the Processor comply with applicable laws, including Data Protection Laws. Furthermore, the Controller shall inform the Processor without undue delay if it is unable to comply with its responsibilities under this section or applicable Data Protection Laws.

3.2. Security Measures. The Controller is responsible for ensuring the secure use of the Services offered by the Processor and must independently determine whether the data security measures provided adequately meet the obligations under applicable Data Protection Laws.

PROCESSOR'S OBLIGATIONS

4.1. Compliance with Applicable Law and Instructions. The 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 Instructions infringe applicable Data Protection Laws (where applicable), it shall inform the Controller without delay. However, such notification shall not constitute a general obligation on the part of the Processor to monitor or interpret the laws applicable to the Controller, nor shall it constitute legal advice to the Controller.

4.3. Conflict of Laws. The Processor will immediately notify the Controller if, for whatever reason, the Controller's request, the Processor will promptly provide reasonable assistance as necessary to enable the Controller to notify the relevant Personal Data Breach to the competent authorities and/or affected Data Subjects, if required under Data Protection Laws.

4.4. Deletion or Return of Personal Data. The Processor will delete or return all Personal Data processed on behalf of the Controller (including copies thereof) upon termination or expiration of the Services provided under the Agreement, within timeframes specified by Controller. As an exception, the Processor may retain part of the Personal Data if required by applicable law.

4.5. Data Protection Impact Assessments and Supervisory Authorities. To the extent that the required information is reasonably available to the Processor, and Controller does not otherwise have access to the required information, the 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), or other competent data protection authorities as required by applicable Data Protection Laws.

DATA SUBJECT REQUESTS

5.1. Assistance with Data Subjects Rights. Considering the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, to fulfill the Controller's obligations, as reasonably understood by the Controller, to respond to requests for the exercise of Data Subject rights under the applicable Data Protection Laws.

5.2. Handling of Data Subject Requests. 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. Engagement. The Controller authorizes to engage Sub-Processors (including Users). When engaging Sub-Processors, the Processor will impose data protection terms on these Sub-Processors that provide at least the equivalent level of protection for Personal Data as those outlined in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. The Processor remains responsible for the compliance of any Sub-Processor with the obligations under this DPA.

6.2. List. The 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 the Processor adds or changes one or more Sub-Processor(s), it will notify the Controller at least 30 days prior to any such change and provide the Controller the opportunity to object to the engagement of the new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 15 days. If the Controller notifies the Processor of such an objection, both parties will discuss the concerns in good faith, aiming to reach a reasonable solution. If no such solution can be reached, the Processor will either not engage the intended new Sub-Processor or allow the Controller to terminate the Service in accordance with the termination provisions of the Service Agreement, without prejudice to any fees incurred by the Controller prior to suspension or termination, but without liability to either party.

6.4. Engagement of Users. The list of Users that were engaged to complete a task of the Controller can be seen using the Toloka Platform interface in the form of hashes assigned to the User(s). The Controller may restrict the engagement of the Users in accordance with the termination provisions of the Service Agreement, without prejudice to any fees incurred by the Controller prior to suspension or termination, but without liability to either party.

6.5. Standard Contractual Clauses. To ensure compliance with Article 46 GDPR, Article 46 UK GDPR and Article 17 of the FADP, the Processor ensures that Standard Contractual Clauses (SCC) will be concluded as applicable. The Standard Contractual Clauses must be incorporated in accordance with Commission Implementing Decision (EU) 2021/914 of 4 June 2021. The Controller and the 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. For Personal Data 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 For Personal Data Subject to the UK GDPR:

i. 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. For Personal Data Subject to the Swiss DPA:

i. 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. Dispute Resolution for SCC: 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.

CONTROLS FOR THE PROTECTION OF PERSONAL DATA

7.1. Protection Measures. The Processor represents and warrants that it has implemented and will maintain all appropriate technical and organizational measures to protect Personal Data Processed hereunder. These measures include 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 Annex III. Upon the Controller's request, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

7.2. Records of Processing. The Processor will duly maintain records of its Processing activities performed on behalf of the Controller.

7.3. Audits and Inspections. Upon prior written request and subject to confidentiality undertakings by the Controller, the Processor shall make available to the Controller (or the Controller's independent third-party auditor, subject to their confidentiality undertakings) all reasonable information necessary to demonstrate compliance with this DPA. The Processor shall also allow and contribute to audits, including inspections, conducted by them. If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 8.5 modifies or alters the Standard Contractual Clauses, nor does it affect any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses. In the event of an audit or inspection, the Processor shall take reasonable steps to avoid causing, or if unavoidable, to minimize, any disruption to the Processor's operations while conducting such audit or inspection.

7.4. Reports. Upon written request by the Controller and limited to once a year, unless substantial elements are indicating the non-compliance by the Processor with the requirements of applicable law and this DPA, the Processor will provide the Controller with a report demonstrating the Processor's compliance with its obligations under this DPA and applicable law.

GENERAL PROVISIONS

8.1. Severability. If any provision of this DPA is found to be invalid or unenforceable, the validity and enforceability of the remaining provisions of this DPA shall not be affected.

8.2. Limitation of Liability. The liability of each Party and their respective Affiliates, in the aggregate, arising out of or in connection with this DPA (including any other DPAs between the parties) and the Standard Contractual Clauses, where applicable, shall be subject to the limitations and exclusions of liability set forth in the Agreement.

8.3. Governing Law. This DPA shall be governed by and construed in accordance with the laws specified in clause 10.1. of the Agreement.

8.4. Disputes. Any dispute arising in connection with this Agreement, which the Parties are unable 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 included in the Customer's dataset and/or are necessary for performing Tasks.

Categories of personal data processed
Any personal data included in the Customer's dataset and/or required for performing 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 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 the 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 duration of the Agreement, plus the period from the expiry of the Agreement until the deletion of the 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 are outlined in Annex IV of the DPA. The duration of the processing by sub-processors corresponds to the duration of the Agreement, unless otherwise agreed 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 I, 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:

The technical and organizational measures to be taken by the Processor to assist the Controller shall provide a level of protection that is essentially equivalent to the measures 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 EU (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:	USA or EU (depends on controller's instructions). East Europe is a default storage location
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):	Data transformation, analytics, batch processing
3 Name:	Google (Google Workspace)
Address:	Google LLC
Hosting location:	EU
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):	Exchanging personal data in inputs and outputs and other documentation necessary for providing Toloka Services (e.g., instructions)
4 Name:	Toloka d.o.o. Beograd
Address:	Starine Novaka 23, Sprat 4, Belgrade (Palilula), 11000, Belgrade, Serbia
Hosting location:	Serbia
Contact person's name, position and contact details:	privacy@toloka.ai
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Support and Maintenance of Toloka Services
5 Name:	Users (as defined in the Agreement) who will be engaged to perform Controller's tasks via Toloka Platform

Previous versions of the document Data Processing Agreement Version 2:

Download