ADDENDUM TO TOLOKA TERMS OF USE OR MASTER SERVICE AGREEMENT FOR THE PROVISION OF TOLOKA SERVICES ("AGREEMENT")

Data Processing Agreement

Last updated: February 07, 2023
Effective Date: February 17, 2023

Terms and definitions

Availability – Ensuring timely and reliable access to and use of information

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Controller (Customer) – Person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body)

Processor (Toloka) – Person, company, or other body which processes personal data on the Data Controller's behalf

Tolokers (Users) – Data subjects who perform tasks placed by Customers

Data subjects – Individual persons whose personal data is collected, held or processed under this Data Processing Agreement. Personal data is any data that can be used to identify an individual, such as a name, addresses, e-mail address, to more obscure information like their ID in service, IP addresses or internet browser data and any other information as defined by applicable law.

Encryption – The process of changing plaintext into ciphertext using a cryptographic algorithm and key

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

Personal data breach – Incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner as defined by applicable law.

Pseudonymisation – Particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. Typically, pseudonymization is implemented by replacing direct identifiers with a pseudonym, such as a randomly generated value.

Resilience – The ability of a party to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats

Sub-processors – Third party data processor engaged by a Data Processor who has or will have access to or process personal data from a Data Controller

1. The Parties hereby enter the contractual clauses between controllers and processors.
2. (a) An entity that is not a Party to these clauses (hereinafter – “Clauses”) may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by adding itself to the Annex and signing this Data Processing Agreement.(b) Once it has added itself to the Annex and signed this Data Processing Agreement, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex.(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.
3. The controller may conduct an inspection at the premises or physical facilities of the processor only subject to a separate agreement with the processor specifying conditions of the relevant inspection.
4. The processor has the controller's general authorization for the engagement of sub-processor(s) from the categories as set forth in 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 the categories of sub-processors at least thirty (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 Parties also agree that the relevant agreed list with the categories of sub-processors is provided in Annex IV to this Data Processing Agreement and may be amended by the processor from time to time.
5. The controller may object to intended changes of the relevant agreed list of sub-processors provided that such objection is based on reasonable grounds relating to data protection by terminating the Agreement immediately upon written notice received by the processor within 20 days as of the controller is informed of the intended changes.
6. 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, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:(a) the pseudonymisation and encryption of personal data;(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
7. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
8. Adherence to a code of conduct or a certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out in Article 6 of this Data Protection Agreement.
9. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by the competent supervisory authorities.
10. In the case of a personal data breach requiring notification under applicable law, the controller shall within the deadline set forth by the law, notify the personal data breach to the competent supervisory authority and/or affected data subjects as required by applicable law. Controller must bear all legal and other fees and expenses that arise out of or relate to the breach notification under this section.Unless otherwise set forth in the applicable law, the notification shall at least:(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;(c) describe the likely consequences of the personal data breach;(d) describe 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.
11. (a) In case of personal data breach requiring notification under applicable law, processor shall notify controller without undue delay upon processor becoming aware of a personal data breach affecting controller's Personal Data, and, at controller's request, provide controller with the requested information in the processor's possession to allow the controller to meet its notice obligations under applicable law.(b) Processor shall co-operate with the controller and take reasonable commercial steps as are directed by controller to assist in the investigation, mitigation and remediation of each such personal data breach.(c) Parties' cooperation in response to a personal data breach will not be construed as an acknowledgement by any party of any fault or liability with respect to the personal data breach.
12. 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 Articles 10-11.
13. Each Party's liability for any breach of this Data Processing Agreement shall be subject to the limitations and exclusions of liability set out in the Agreement, provided that neither Party limits or excludes any liability that cannot be limited or excluded under applicable law.
14. All references of this Data Processing Agreement to requirements of data protection laws of shall be read as references to relevant requirements of applicable data protection laws, including, without limitation, data protection laws of the Data subjects' states of residence.
15. Annexes I – IV are attached to this Data Processing Agreement.

ANNEX I

List of parties

Controller: 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.

Processor: Toloka AI Inc10 State street, Newburyport, MA 01950, United StatesContact email: 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 Tolokers performing Tasks

Categories of personal data processed

Any personal data contained in Customer's dataset and/or personal data of Tolokers 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 specialized 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 sensitive personal data of Tolokers performing Tasks. Strict purpose limitation and access restrictions are employed.

Nature of the processing

The processor provides the controller with Services specified in the Toloka Terms of Use and/or Master Services Agreement. The processor performs on behalf of the controller operations on personal data as required to provide the service: Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure, and destruction. Upon request of the controller the processor may store Tolokers' consents.

Purpose(s) for which the personal data is processed on behalf of the controller

- Execution of tasks by Tolokers;
- Execution of tasks by Tolokers, which, at the request of the Customer, may contain Personal Data (PD);
- Communication between the Customer and Toloker, when the Toloker performs tasks for this Customer.

Duration of the processing

Term of the Service under Toloka Terms of Use or Master Services Agreement entered by the parties plus the period from expiry of the term until deletion of the data by the processor in accordance with this Data Processing Agreement.

Transfer of personal data

Party/Third-party	Role in process	Purpose of transfer	Operations on personal data	Duration of processing
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	**Controller**	Execution of tasks by Tolokers; Execution of tasks by Tolokers, which, at the request of the Customer, may contain PD; Communication between the Customer and the Toloker, when the Toloker performs tasks for this customer	Collection, recording, storage, destruction, adaptation or alteration, erasure, transfer (distribution, provision, access)	Duration of the agreement on provision to the controller of the Service under the Toloka Terms of Use 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
IT providers	**Sub-processor**	Maintenance of the software/hardware/ technical infrastructure used for provision of the Services to the controller under Toloka Terms of Use or Master Services Agreement	Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure, and destruction	Duration of the agreement on provision to the controller of the Service under the Toloka Terms of Use 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
Hosting providers	**Sub-processor**	Data center services	Storage, erasure, and destruction	Duration of the agreement on provision to the controller of the Service under the Toloka Terms of Use 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

Territorial Restrictions:

Controller may restrict the region of Tolokers (Users) for performance of its tasks via the tools of the Platform.

ANNEX III

Technical and organizational 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:

- TLS is used to protect data during transmission. TLSv1.3 is supported.
- 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 ISO 27001 and ISO 27701.
- Backups are performed daily.
- Physical security. Only authorized personnel have access to the premises. Access is managed with access control systems and video surveillance.
- 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 Physical 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

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

Category of sub-processor	Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorized)
Service developers	Processing required for maintenance of the software/hardware/technical infrastructure used for provision of the Services under Toloka Terms of Use or Master Service Agreement entered by the parties.
Data centers	Processing required for provision to the processor of data center services.
Retained Tolokers (Users) (as defined in the Agreement)	Processing required to perform Controller's tasks via Toloka platform

Previous versions of the document: https://toloka.ai/legal/dpa_usa/01082022