Privacy & AI Transparency Notice

Date of effect: Sep 10, 2026
Last updated: Sep 10, 2026

We have developed this Privacy Notice (“Privacy Notice”) to explain to you how we collect, use, disclose, and store personal data. Toloka may update this Privacy Notice at any time and you are encouraged to return to this page to remain current with our notice.

Introduction

This Privacy Notice applies to Toloka AI B.V. and its relevant affiliates listed in Section 16 (“Toloka”, “we”, “us”, “our”).

When Does This Privacy Notice Apply?

This Privacy Notice applies to personal data that Toloka handles as a Controller, including when you:

- Visit or interact with the toloka.ai, we.toloka.ai and/or mindrift.ai websites (the “Website(s)”), the Toloka Platform, the Toloka, Toloka: Annotators and Mindrift mobile applications, other resources associated with Toloka, and the branded social media pages we operate;
- Register for or participate in our webinars, events, programs, marketing initiatives, and promotional activities;
- Interact with us in person, such as when you visit our offices; and
- Inquire about or engage in commercial transactions with us.

After reviewing this Privacy Notice, please check the country-specific provisions at the end of this Privacy Notice, which may apply to the processing of your data based on your country of residence. These provisions either supplement this Privacy Notice or, if required by law, take precedence over any conflicting terms.

This Privacy Notice refers to provisions of:

- General Data Protection Regulation (GDPR);
- Serbian Law on Personal Data Protection (2018);
- US privacy legislation (including but not limited to the California Consumer Privacy Act (CCPA), the California Privacy Rights Act of 2020 (CPRA), the California Online Privacy Protection Act (CalOPPA), the Virginia Consumer Data Protection Act (CDPA), the Colorado Privacy Act (CPA), the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA), the Utah Consumer Privacy Act (UCPA), and, where applicable to children's data, the federal Children's Online Privacy Protection Act (COPPA)); and
- other applicable laws in force as of the last update of this Privacy Notice.

1. Controller

Toloka is the controller of the personal data processed under this Privacy Notice. This means that Toloka determines the purposes and means of processing this personal data.

Toloka has appointed a data protection officer who may be contacted at privacy@toloka.ai with any questions regarding the processing of your personal data.

2. Legal bases

Depending on which features of Toloka you use, we process your personal data based on one or more of the following legal bases:

Contract

To fulfill our contractual obligations to you and provide access to the Toloka Platform, we may process your personal data. This includes activities such as account registration and money withdrawal.

Legitimate interest

When Toloka has a legitimate interest in using your personal data in a certain way, provided that such use is necessary and justified given any potential risks to you, we first conduct a Legitimate Interest Assessment (LIA) to ensure your personal data is adequately protected. This includes verifying the identity of individuals acting on behalf of our vendors, suppliers, customers, and other business counterparties (for example, authorized signatories, directors, or beneficial owners) as part of our standard fraud-prevention and counterparty due-diligence process.

Consent

When Toloka requests your consent to process your personal data for specific purposes. Where personal data processing is based on your consent, you have the right to withdraw your consent at any time; withdrawal does not affect the lawfulness of processing carried out before the withdrawal. To withdraw consent, contact us using the details in Section 1.

Explicit consent (special category data)

Where our identity-verification process includes biometric processing (for example, matching a live photo against a government-issued ID), we rely on your explicit consent for that biometric processing. You may withdraw this explicit consent at any time using the contact details in Section 1.

Legal obligation

Toloka may also be required to process or share your personal data with competent authorities in accordance with applicable legislation,, for example, reporting certain identity, address, and tax-identifier information to tax authorities for EU platform workers under the EU's DAC7 reporting directive. Where we rely on this legal basis, you do not have a right to withdraw, and we cannot delete this data before the legally required

retention period ends (see Sections 5 and 6).

Providing your data

Where indicated in Section 3, providing certain personal data is necessary to enter into or perform our contract with you or to meet our legal obligations. For example, account-registration data is required to create and operate your account, and identity-verification data (including biometric data processed with your consent) is required for us to meet sanctions-screening and tax obligations. If you do not provide this data, we may be unable to create your account, verify your identity, process payments, or allow you to work with or through the Toloka or Mindrift platforms, or, where you act on behalf of a vendor, customer, or other business counterparty, complete our onboarding of that counterparty or enter into or continue the applicable agreement.

3. How We Process Your Personal Data

This section describes, by category of activity, the personal data we process, why we process it, the legal basis we rely on, and the categories of organizations we may share it with.

Where personal data is obtained from third parties rather than directly from you, our common sources include referrals from other users, publicly available professional profiles (e.g., LinkedIn, Indeed) where you apply for a role, and the service providers described below.

Some of the processing activities below are carried out by Toloka affiliates acting as joint controllers; others involve affiliates or service providers acting as processors on our behalf. Where affiliates act as joint controllers, the essence of the arrangement between them — including which affiliate is responsible for which obligation — is available on request by contacting privacy@toloka.ai.

Account and platform operations

We process account holder data (such as name, email, date of birth, username, phone number, country, and language/education preferences relevant to task eligibility) to create and manage your account, authenticate you, pay you, and provide customer support. Legal basis: contract with you; legitimate interest in maintaining accurate account and support records, preventing and detecting fraud, and compliance with contracts and laws or regulations. Categories of recipients: cloud infrastructure and identity providers; payment and payout processors; customer support platforms and compliance service platforms and providers; Toloka affiliates (as joint controllers for shared account infrastructure).

Communications, marketing, and events

We process contact details (name, email, company, job title) of newsletter subscribers, webinar/event registrants, and prospective customers or experts to send communications, administer events, and market our services. Legal basis: consent for newsletters and

marketing communications; legitimate interest in maintaining business relationships and records; contract where communications relate to a transaction. Categories of recipients: email and marketing platform providers; customer relationship management providers; scheduling and video-conferencing providers.

Website and product analytics

We process device, browser, IP address, and usage data from website visitors and platform users to understand how our sites and products are used and to improve them. Legal basis: consent for non-essential analytics and advertising cookies; legitimate interest in the proper functioning and security of our websites and platform (see our Cookie Notice for details on each category of cookie and how to manage your preferences). Categories of recipients: web analytics providers; advertising and social media platforms (where you have consented); cloud data-warehouse providers.

Trust, safety, and fraud prevention

We process account, device, and interaction data to detect and prevent fraudulent activity on the platform, and may restrict access where fraud is suspected or confirmed (see Section 8 for more on this automated process). Legal basis: legitimate interest in preventing fraudulent activity and protecting the platform and its users as well as compliance with contracts and applicable laws. Categories of recipients: identity and background check service providers; cloud data warehouse providers; Toloka affiliates (as joint controllers).

Identity verification and sanctions/compliance screening

We process government-issued ID, date of birth, geolocation and, where our verification process includes a biometric facial match, biometric data (such as a live photo compared against a government-issued ID) to verify identity and automatically screen against applicable sanctions and compliance requirements before onboarding certain account holders, customers, suppliers, or other business counterparties (including individuals acting on their behalf, such as authorized signatories, directors, or beneficial owners). Where our verification process includes biometric processing, we rely on your explicit consent for that processing, and you may decline or withdraw it; however, identity verification is necessary for us to meet our legal sanctions-screening obligations and, in some cases, our contractual obligations to the counterparty you represent, so if you do not provide it we will be unable to onboard you, the counterparty you represent, or continue the applicable engagement. Legal basis: our legitimate interest in preventing fraud and verifying the identity of our counterparties and their representatives; your explicit consent, where our verification process includes biometric processing; legal obligation for sanctions screening required by applicable law. Categories of recipients: identity-verification providers; sanctions-screening and compliance-data providers.

Contracting, payments, and tax/legal compliance

We process account, company, and payment-related data (bank/e-wallet details, transaction data, tax identifiers, and, for EU-based Tolokers and Experts, full postal

address, place of birth, tax identification number (TIN) and issuing member state, and VAT ID) to enter into and administer contracts with Tolokers, Experts, contractors, customers, and suppliers, and to meet our financial, tax, and legal record-keeping obligations. Legal basis: contract; legal obligation for tax and accounting recordkeeping; legitimate interest in financial and legal recordkeeping. Categories of recipients: payment and payout processors; e-signature and contract-management providers; Toloka affiliates (as joint controllers); and tax authorities where required by law

Recruitment and freelance onboarding

We process CV, education, work-history, and (where applicable) AI-assessed interview data to evaluate candidates for freelance positions and AI Tutor roles. This includes using third-party recruitment services that apply AI to their candidate pools to identify and proactively contact potential candidates (meaning we may obtain your data from these platforms even if you have not applied to us directly), AI-assisted checks of submitted CVs for fraud or discrepancies, AI-assisted screening, and, where used, third-party AI interview platforms (see Section 8).

Reviews, ratings, referrals, and surveys

We process name, email, and feedback content from account holders who choose to leave a public review or rating, participate in our referral program, or take part in surveys. Legal basis: consent. Categories of recipients: review-platform and referral-platform providers, which may act as independent controllers for content you choose to publish.

Communication tools (Discord, Telegram, and similar)

Where you choose to communicate with us through Discord, Telegram, or similar third-party platforms, we process your username, profile information, and messages exchanged through that platform. Legal basis: consent; legitimate interest in facilitating platform-related communication. Categories of recipients: the relevant messaging platform, under its own privacy policy.

Software engineering and coding task deliverables

We process the name, email address, usernames, and handles (for example, Slack, Jira, Git*, etc.) of individuals who contribute to software engineering and coding tasks — including both external experts/contributors and Toloka's internal team members — where that data appears in code commit or authorship metadata, in other in-repository content, in mocked Slack, Jira, or document data delivered with a task (including @-mentions and reporter/assignee/author fields), or in task annotations and preference labels submitted alongside the work. This applies only to specific client projects that involve delivery of coding/software-engineering task outputs. Clients receiving these deliverables (e.g., code repositories, commits, and associated task materials) may use this information as part of developing, evaluating, or training AI models. Legal basis: legitimate interest in delivering the contracted work product in the form it was created and in enabling the client's development, evaluation, and training of its AI systems. Categories of recipients: the applicable client and its approved processors/affiliates.

4. Transfers to third countries

Toloka transfers personal data to countries that may not provide the same level of data protection as the EU, UK, or Switzerland ("Third Countries").

To protect your data in such transfers we use one or more of: Standard Contractual Clauses (SCCs) adopted by the European Commission; the EU–US/UK–US/Swiss–US Data Privacy Framework (DPF) where the recipient is certified; Binding Corporate Rules (BCRs) when available; adequacy decisions; or other approved transfer mechanisms, together with supplementary technical and organizational measures where appropriate.

For transfers of personal data originating in Serbia, Toloka relies on the standard contractual clauses issued by the Serbian Commissioner for Information of Public Importance and Personal Data Protection, the Serbian Government's adequacy list, or the Commissioner's specific approval, as applicable, in addition to the EU mechanisms described above.

We also apply technical safeguards, including encryption in transit and at rest, to further protect your personal information.

5. How Long We Keep Your Data

This section explains the criteria we use to decide how long each category of data is kept — consistent with the data-minimization and storage-limitation principles of the laws referenced in this notice.

In general, when data is no longer needed we delete or anonymize it so it no longer identifies you. We determine how long to keep each category of data using the following criteria:

- Contract and account data (e.g., registration and profile information): kept for as long as your account or contract is active, plus a defined period afterward tied to the statute of limitations for contract-related claims and to applicable tax and accounting record-keeping law in the relevant jurisdiction (Netherlands, United States, or Serbia).
- Consent-based data (e.g., newsletters, marketing communications, non-essential cookies): kept until you withdraw consent, or until a defined period of inactivity is reached, whichever comes first.
- Biometric and identity-verification data: kept no longer than three (3) years or the term of the applicable Agreement, whichever is shorter — consistent with statutory retention-schedule requirements applicable to biometric data (e.g., the Illinois Biometric Information Privacy Act) — unless you give explicit written consent to a longer period.
- Fraud-prevention and security data: kept only as long as needed to detect, investigate, and resolve suspected fraud or security incidents, benchmarked to our incident-response and investigation cycles.
- Legal-obligation data (e.g., sanctions screening, tax reporting): kept for the period required by the specific law that obligates its collection, plus a defined buffer to

respond to related regulatory inquiries.
- Dispute and claims-related data: kept until the applicable limitation period for the relevant legal claim has passed.
- Client-delivered software engineering/coding task data (e.g., commit metadata, mocked Slack/Jira/document content, and task annotations containing contributor identifiers): kept per the applicable project/client agreement.

6. Your rights

You have the following rights. To exercise them, contact Toloka using the details in Section 1. We may ask you to submit your request in writing and to verify your identity before processing it, and we may decline requests where permitted by law.

- Access — ask us to confirm whether we hold your data and receive a copy of it.
- Rectification — ask us to correct or complete inaccurate or incomplete data.
- Erasure (‘right to be forgotten’) — ask us to delete your data where it is no longer needed, processed unlawfully, or where you have withdrawn consent and no other legal basis applies.
- Restriction on processing — ask us to pause processing while a request is disputed, when processing is unlawful but you prefer restriction over deletion, or while an objection is considered.
- Objection to processing — object to processing based on legitimate interests (including direct marketing). We will stop unless we have compelling legitimate grounds that override your interests.
- Data portability — where processing is based on your consent or a contract with you and the data collection and format is applicable, receive your personal data in a structured, commonly used, machine-readable format, and ask us to transmit it directly to another controller where technically feasible.
- Withdraw consent — where processing is based on consent or explicit consent, withdraw it at any time without affecting the lawfulness of prior processing.

7. Children's Privacy

Our services are not directed to individuals under 18. If you are under 18, do not register or provide personal data without parental or guardian consent. If you believe a child has provided data without proper consent, contact us at privacy@toloka.ai and we will delete it promptly.

We do not collect personal data from children under 18 except in the context of a Toloka Study, which requires explicit written parental or guardian consent. Parents and guardians may request access to, correction of, or deletion of their child's data by contacting us.

Separately, where any Toloka Study involves personal data from a child under 13 in the United States, we comply with the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §6501 et seq., including obtaining verifiable parental consent before collecting such

data.

In accordance with 47 U.S.C. §230(d), we note that parental control software is commercially available to limit minors' access to online services.

8. Profiling and automated decision-making

As part of its personal data processing activities, Toloka may perform profiling and automated decision-making for two purposes: (1) to monitor user behavior on the Toloka platform for fraud prevention and detection, and (2) in recruitment, to (a) identify and proactively contact potential candidates from third-party talent pools, (b) verify submitted CVs for fraud or discrepancies, and (c) assist in screening candidate CVs and conducting AI-supported interviews to evaluate whether a candidate's experience and skills meet role requirements.

(1) Profiling and automated decision-making for anti-fraud purposes are conducted through Toloka's anti-fraud system, which analyzes data collected from user activities on the Toloka platform. If fraudulent activity is detected, the anti-fraud system may immediately restrict the user's access to task submissions, terminate agreements related to tasks, or, if the fraudulent activity is identified from the task requester's account, restrict their access to Toloka. If fraudulent activity is detected but an investigation does not confirm fraud and your identity is successfully verified, your access may be restored; if fraud is confirmed or you are unable to verify your identity, your access will remain restricted.

AI-assisted hiring

During recruitment, Toloka uses AI tools to help identify and contact potential candidates from third-party talent pools, to check submitted CVs for fraud or discrepancies, and to assist our recruiters in reviewing candidates, and we may invite candidates to an AI-supported interview on a third-party platform. AI outputs inform, but do not replace, human judgment: a member of our recruitment team has the authority to reach a different outcome before any hiring decision is made.

You have the right to: (a) object to profiling or automated decision outcomes; (b) request a clear and meaningful explanation of the role the AI system played in the decision-making procedure and the main elements of the decision taken about you; (c) request further information about the logic involved; and (d) request human review of any automated decision, including the right to express your point of view and contest the outcome. To do so, contact Toloka via https://mindrift.zendesk.com/hc/en-us. We will ask you to verify your identity and may ask you to specify your request in writing. We will respond within one month of a verified request.

9. Supervisory Authority Complaints

You have the right to lodge a complaint with a supervisory authority, including:

- EU residents: the supervisory authority in your EU member state of residence. As

Toloka AI B.V. is established in the Netherlands, the lead EU supervisory authority is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

- Serbian residents: Commissioner for Information of Public Importance and Personal Data Protection (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti) — www.poverenik.rs.

10. Principles of data security

Toloka maintains an Information Security Management System (ISMS) and Privacy Information Management System (PIMS) certified under ISO/IEC 27001 and ISO/IEC 27701, respectively, audited annually by an independent external auditor. Where a personal data breach affecting your personal data occurs, we will notify affected individuals and the relevant supervisory authority to the extent, and in the manner, required by the applicable law of your jurisdiction. To report a security incident, contact security@toloka.ai.

11. Cookies

We use cookies and similar tracking technologies on our Websites. You can manage your cookie preferences via the “Manage Cookies” link in our Website footer or your browser settings. For full details, see our Toloka Cookie Notice (toloka.ai) and Mindrift Cookie Notice (mindrift.ai).

12. This Privacy Notice and Links to Other Sites

Our Websites may link to third-party sites not operated by Toloka. This Privacy Notice does not apply to those sites. We recommend reviewing each site's own privacy policy. We take no responsibility for the content or privacy practices of third-party sites.

13. Difficulty Accessing this Privacy Notice

If you cannot access this Privacy Notice online, contact us at privacy@toloka.ai to request it in an alternative format. We will not collect or process sensitive data in connection with such a request.

14. State/Country specific Privacy Policies and Notifications

United States of America

A. Privacy Information for California Residents

This section applies only to California residents and prevails over other parts of this Privacy Notice in case of any discrepancy. Personal information has the same meaning as personal data in this section.

Personal information we collect, the sources, and the purposes are described in Section 3 above. We do not sell your personal information to third parties. “Sale” does not include

transfers of personal information as part of a merger, acquisition, or other business transaction; if such a transaction materially affects how your personal information is processed, we will notify you before the change takes effect.

Your California Privacy Rights

In addition to the rights in Section 6, California residents may:

- request, at no charge, the categories and names/addresses of third parties that received your personal information for direct marketing purposes;
- upon a verifiable request, obtain the categories of personal information collected, sold, or disclosed for a business purpose, the categories of sources, the business/commercial purpose, and the categories of third parties with whom it is shared;
- opt out of the sale of personal information (we do not currently sell personal information); and
- exercise these rights without discrimination in the services or quality of service you receive from us.

To submit a verifiable request, contact us using the details in Section 1. We will ask you to provide information to verify your identity, which may include your name, address, email address, and your account ID with Toloka. An authorized agent may submit a request on your behalf but must identify you, provide proof of authorization, and, in most cases, your written consent confirming the agent's authority.

Removal of Minor Information

A parent or guardian may request removal of information about a minor by emailing us with the subject line “Removal of Minor Information,” including the nature of the request, the content/location to be removed, and the parent/guardian's contact details. Minors themselves may not submit such requests.

Do Not Track

We do not support Do Not Track (DNT) signals under the California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §22575 et seq. Third parties may still collect data about you; we cannot control their response to DNT signals, which is governed by their own privacy policies.

B. Privacy Information for Residents of Colorado, Connecticut, Utah, Virginia, and Nevada

Unless otherwise stated by the law of your state of residence, the provisions in Section A above apply to the processing of your data.

Right to appeal (Colorado, Connecticut, Virginia): if we decline to act on your request, you may appeal our decision by contacting us using the details in Section 1. We will respond to your appeal within sixty (60) days. If you disagree with the outcome, Colorado and

Connecticut residents may contact their state Attorney General, and Virginia residents may contact the Virginia Attorney General's Office.

Colorado residents have the right to opt out of processing for targeted advertising or the sale of personal data. We do not currently recognize an automated universal opt-out mechanism such as Global Privacy Control; we are working to support one. In the meantime, you may exercise your opt-out rights by contacting us using the details in Section 1 or through the cookie-preference controls described in Section 11.

15. Changes to this Privacy Notice

Toloka may update this Privacy Notice from time to time, at its discretion. When changes are made, we will take reasonable steps to notify you about the changes and their effects, using appropriate methods and providing timely notice.

We recommend that you regularly review this Privacy Notice, located at the footer of the Website, and check for updates, especially when becoming aware of any changes. Updates will be reflected in the revised Privacy Notice and the “last updated” date at the top of this page.

Changes take effect on the “Date of Effect,” which will be no earlier than the date they are posted on this page.

In the event of discrepancies between the English version of this Privacy Notice and any translation, the English version takes precedence.

16. Affiliates

TOLOKA GROUP, INC. (USA), 1604 Philadelphia Pike PMB 117, Wilmington, DE 19809

TOLOKA AI, INC. (USA), 1604 Philadelphia Pike PMB 117, Wilmington, DE 19809

TOLOKA D.O.O. BEOGRAD (SRB), registration number: 21804126, registered address: Starine Novaka 23, Sprat 4, Belgrade (Palilula), 11000, Belgrade, Serbia

Toloka AI B.V., registration number: 82041350, registered address: Claude Debussylaan 7, 1082MC Amsterdam