TikTok US Applicant Privacy Notice

Last Updated: February 28, 2024

TikTok ("**we**" or "**us**") has prepared this Applicant Privacy Notice ("**Notice**") for those applying to roles at TikTok (**"job applicants", "potential candidates"** and/or **"you"**/ **"your"**). This Notice describes how we handle and protect the personal data of job applicants and potential candidates in connection with our recruiting processes and programmes. It is important that you understand who we are, how we use your personal data and that we take our obligations very seriously. The purpose of this Notice is to give you information about how TikTok collects, processes, stores and otherwise uses your personal data and your rights in relation to that data.

TikTok needs to process your personal data in order to process your application for employment. There may also be statutory requirements we have to comply with in relation to your application. If we are not able to carry out the processing activities we describe in this Notice we may not be able to continue with your application.

For the purposes of this Notice, references to "TikTok" comprises the following U.S. entities: TikTok Inc., ByteDance Inc., Lark Enterprise Applications Inc., and any US incorporated affiliates.

In addition, you will see several references to the "TikTok Group", which includes all other TikTok entities globally. As with many other TikTok policies, we may update this document from time to time, for example if we implement new systems or processes that involve the use of personal data. Any material updates to this document which may affect you will be communicated to you through appropriate channels, such as on the TikTok job applicant site or via TikTok's communication tools.

Index

To help you find information on any particular question you might have, we have set out an index below:

- What categories of personal data does TikTok collect about me?
- What are the sources from which TikTok collects personal information about me?
- For what purposes does the Company need my applicant personal data?
- Who might TikTok disclose my personal data to?
- How long will TikTok retain my personal data?
- Privacy rights for California residents and how to exercise them.
- Who can I contact about this Notice?

What categories of personal data does the Company collect about me?

TikTok may collect, process and use the following categories and types of personal data about you when you apply for a job:

- **Identifiers**, such as real name, nickname or alias, postal address, telephone number, e-mail address, Social Security number, signature, online identifier, driver's license number or state identification card number, gender, birthday, nationality, immigration or visa number, and passport number;
- **Paper and electronic records that contain personal data**, name, signature, photo, physical description, application and interview responses, applicant feedback and survey responses regarding the recruiting process or applicant portal, financial or payment information (e.g., bank account name and number for direct deposits), insurance information (e.g., insurance policy number and information), and medical information (e.g., information and records necessary for occupational health surveillance, occupational health and safety compliance and record-keeping, to conduct fitness-for-duty examinations, and information necessary to respond to an applicant's medical emergency);
- **Characteristics of protected classifications**: such as race, national origin, disability, sex, and veteran status, religious, philosophical or political beliefs, and other characteristics of protected classifications under state or federal law, such as information necessary to comply with the reporting requirements of the federal Equal Employment Opportunity Act and the federal Office of Contracting Compliance Programs (applicable to government contractors). *Note: this information is generally only collected on a voluntary basis and is used in support of our equal opportunity and diversity and inclusion efforts within the Company, as well as for our legal reporting obligations, or where otherwise required by law*;

- **Internet or other electronic network activity information**, such as browsing history, Internet Protocol address, search history, and information regarding an applicant's interaction with Company electronic resources, websites, application, or other online services, as well as physical and network access logs and other network activity information related to your use of any Company electronic resources;

- **Audio, video and other electronic data**, such as audio, electronic, visual, or similar information, such as CCTV footage, photographs, and call recordings and other audio recording (e.g., recorded meetings and webinars)

- **Employment information**, such as professional or employment-related information, including evaluations, membership in professional organizations, professional certifications, and employment history;

- **Education information**: information about education history or background, such as academic transcripts, educational discipline records, and academic counseling records;

What are the sources from which TikTok collects personal information about me?

- **Directly from you**, for example, in your job application, forms you fill out for us, assessments you complete, and any information you provide us during the course of your application and interview process.

- **Vendors and service providers**, for example, recruiters.

- **Third parties**, for example, job references, affiliated companies, professional employer organizations or staffing agencies.

- **Public internet sources**, for example, social media, job boards, public profiles, and other public online sources.

- **Public records,** for example, court records.

- **Automated technologies** on TikTok's electronic resources, for example, to track logins and activity on Company's career page.

- **Surveillance/recording technologies installed by Company**, for example, video surveillance in common areas of Company premises, voicemail technologies, webcams, and audio/video recording technologies with consent andto the extent required by law.

- **Government or administrative agencies**, for example, law enforcement or public health authorities.

Note: This Privacy Policy does not cover background screening conducted by third-party background check vendors subject to the federal Fair Credit Reporting Act. TikTok provides a separate disclosure for such screening.

For what purposes does the Company need my applicant personal data?

Generally, we may use and disclose the above categories of personal data for the following business purposes:

- **Recruiting, hiring and managing, and evaluating Applicants.** To review, assess, recruit, consider or otherwise manage applicants and job applications, including:
- To evaluate applicants' qualifications for employment with the Company
- To communicate with applicants
- For diversity and inclusion purposes within the Company as well as related to reporting obligations
- To create a talent pool for future job openings
- To arrange and manage Company-sponsored events
- For recordkeeping purposes, such as to demonstrate applicants' agreement to, or acceptance of, documents presented to them, e.g., pre-employment arbitration agreement, acknowledgement of employment application, offer letter
- To evaluate and improve the recruiting process, such as by requesting feedback through surveys about the recruiting process or our applicant portal
- Scheduling and conducting interviews
- Identifying applicants, including by working with external recruiters
- Reviewing, assessing and verifying information provided, to conduct criminal and background checks (where relevant and pursuant to applicable law), and to otherwise screen or evaluate applicants' qualifications, suitability and relevant characteristics
- Extending offers, negotiating the terms of offers, and assessing salary and compensation matters
- Satisfying legal and regulatory obligations
- **Security and Monitoring.** In order to monitor and secure our resources, network, premises and assets, including securing our offices, premises and physical assets, including through the use of electronic access systems and video monitoring

- **Health and Safety**. For health and safety purposes, such as:
  - To conduct fitness-for-duty examinations
  - Conducting appropriate health and safety screenings of individuals prior to entering or accessing certain locations or premises
  - For occupational health surveillance and occupational health and safety compliance and record-keeping
  - As otherwise necessary to protect the health and safety of applicants, personnel and visitors to our premises
- **Compliance with Applicable Legal Obligations.** Relating to compliance with applicable legal, regulatory, ethical and corporate responsibility obligations, such as:
  - Administering the Company's complaint processes and procedures
  - Reporting suspected criminal conduct to law enforcement and cooperating in investigations
  - Responding to subpoenas and court orders
  - Conducting assessments, reviews and reporting relating to our obligations, including under employment and labor laws and regulations, social security and tax laws, environmental regulations, workplace safety laws and regulations, and other applicable laws, regulations, opinions and guidance.
- **Improving and evaluating our recruiting process**. To evaluate and improve our recruiting process, including in support of meeting our diversity and inclusion efforts and for candidates the opportunity to self-identify.
- **Auditing, Accounting and Corporate Governance**. Relating to financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations, and for other internal business purposes such as administration of our records retention program.
- **M&A and Other Business Transactions**. For purposes of planning, due diligence and implementation of commercial transactions (e.g., mergers, acquisitions, asset sales or transfers, bankruptcy or reorganization or other similar business transactions).
- **Defending and Protecting Rights**. In order to protect and defend our rights and interests and those of third parties, including to manage and respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health or safety of others, including in the context of anticipated or actual litigation with third parties.

No sales or "sharing", *i.e.*, disclosure for cross-context behavioral advertising:

TikTok does not sell the personal data of any applicants or share their personal data for cross-context behavioral advertising.

Who might TikTok disclose my personal data to?

As you may know, the TikTok entity to which you are applying for a role is part of the global TikTok Group, with offices located across the globe, which support HR administration and provide services such as cloud storage, research and development, analytics and security.

TikTok may disclose your personal data to third parties outside of the TikTok Group. The types of third parties to which we disclose your data, and the reasons why we disclose it, are as follows:

- **Regulators, authorities, business partners and other third parties**. We may need to disclose your personal data to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), independent external advisors (e.g., auditors, accountants, lawyers and consultants), insurance, pensions and benefits providers (for successful applications), internal compliance and investigation teams (including external advisers appointed to conduct internal investigations).

- **Acquiring entities.** If the TikTok business to which you are applying to is sold or transferred in whole or in part (or such a sale or transfer is being contemplated), your personal data may be transferred to the acquiring entity as part of the transfer itself or as part of an initial review for such transfer (i.e. as part of any due diligence). This is subject to any rights provided by applicable law, including jurisdictions where the acquiring entity is located.

- **Service providers acting on behalf of TikTok.** As necessary for the purposes of processing listed above, your data may be disclosed to third parties to process under appropriate instructions and on behalf of the relevant TikTok entity ("Data Processors"). Data Processors may carry out instructions related to applicant data administration including, where applicable, external recruitment agencies and recruitment system providers (including support and maintenance), payroll, compensation & benefits (for successful applicants), training, health and safety, compliance, photography and videography, and other activities. Data Processors are subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard personal data and to process it only as instructed.

For more information on the parties to which we disclose your personal data, and where it is transferred to, you can contact us through the email provided below.

Some of the third-party recipients to which we may disclose applicant data may be located in countries outside of the country where you apply.

For transfers to TikTok Group entities outside of the country where you apply (an "International Transfer"), and International Transfers to third parties, TikTok takes all necessary measures to ensure your personal data is adequately protected. This includes using appropriate transfer mechanisms and contractual clauses.

How long will TikTok retain my personal data?

It is TikTok's policy not to store personal data for longer than is necessary, and to retain such data only on a basis proportionate to achieving the purposes prescribed above. This means that TikTok retains personal data for: (i) the period of time required for the purposes for which it was collected; (ii) any compatible and lawful purposes subsequently established; (iii) any new purposes to which you subsequently consent; and/or (iv) compliance with legal and regulatory requirements.

Privacy Rights for California Residents And How To Exercise Them

Your California Privacy Rights

- **Right to Know**: You have the right to submit a verifiable request to know specific pieces of your personal information obtained from you and for information about Company's collection, use, and disclosure of your personal information. Please note that the CPRA's right to obtain copies does not grant a right to the whole of any document that contains personal information, but only to "specific pieces" of personal information. Moreover, you may have a right to know categories of sources of personal information and categories of external recipients to which personal information is disclosed, but not the individual sources or recipients.

- **Right to Delete**: You have the right to submit a verifiable request for the deletion of personal information that you have provided to TikTok.

- **Right to Correct**:You have the right to submit a verifiable request for the correction of inaccurate personal information maintained by TikTok, taking into account the nature of the personal information and the purposes of processing the personal information.

How to Exercise Your Rights

TikTok will respond to requests to know, delete, and correct in accordance with applicable law after it can verify the identity of the individual submitting the request. You can exercise these rights in the following ways:

- Using This Webform:

- Emailing us at **hrdataprotection@tiktok.com**

How We Will Verify Your Request

The processes that we follow to verify your identity when you make a request to know, correct, or delete are described below, and depend on how and why the request is submitted.

If you submit a request by any means other than through a password-protected account that you created before the date of your request, the verification process that we follow will depend on the nature of your request as described below:

1. **Requests To Know Categories or Purposes:** If you request to know how we collect and handle your personal information, we will match at least two data points that you provide with your request, or in response to your verification request, against information about you that we already have in our records and that we have determined to be reliable for purposes of verifying your identity. Examples of relevant data points include your mobile phone number, your zip code, and the month and year you submitted a job application to us.

2. **Requests To Know Specific Pieces of Personal Information:** We will match at least three data points that you provide with your request to know, or in response to our request for verification information, against information that we already have about you in our records and that we have determined to be reliable for purposes of verifying your identity. In addition, we may require you to sign a declaration under penalty of perjury that you are the individual whose personal information is the subject of the request.

3. **Requests To Correct or Delete Personal Information:** Our process for verifying your identity will depend on the risk level (as determined by Company) associated with the personal information that you ask us to correct or delete. For low risk personal information, we will require a match of two data points as described in Point No. 1, above. For higher risk personal information, we will require a match of three data points and a signed declaration as described in Point No. 2, above.

We have implemented the following additional procedures when verifying the identity of requestors:

1. If we cannot verify your identity based on the processes described above, we may ask you for additional verification information. If we do so, we will not use that information for any purpose other than verification.
2. If we cannot verify your identity to a sufficient level of certainty to respond to your request, we will let you know promptly and explain why we cannot verify your identity.

Authorized Agents

If an authorized agent submits a request to know, correct, or delete on your behalf, the authorized agent must submit with the request a document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you or your authorized agent to follow the applicable process described above for verifying your identity. You can obtain the "Authorized Agent Designation" form by contacting us at hrdataprotection@tiktok.com

TikTok's Non-Discrimination and Non-Retaliation Policy

TikTok will not unlawfully discriminate or retaliate against you for exercising your privacy rights under the California Privacy Rights Act.

Who can I contact about this Notice?

If you have concerns or questions regarding this Notice or our handling of your personal data, you can contact us at hrdataprotection@tiktok.com.