PRIVACY NOTICE FOR JOB CANDIDATES

[Last Updated: January 2026]

This job candidates' privacy notice ("**Candidates Privacy Notice**") describes what Personal Data (as defined below) Kaltura Group[1] (collectively "**Kaltura**", "**we**" or "**us**" or "**our**") collect and process about individuals who apply for positions we offer ("**Candidates**", "**you**" or "**your**") during the recruitment process and, where relevant, afterwards. This Candidates Privacy Notice applies to Candidates in the territory where we offer job opportunities and is subject to applicable data protection laws ("**Data Protection Laws**").

This Candidates Privacy Notice applies to the processing, sharing, and storing of Personal Data (as defined below) during and after the recruitment process. It is provided in addition to, and does not replace, any privacy policies that govern the use of our website and services.

This Candidates Privacy Notice describes Kaltura's data privacy and security practices in the recruitment context, including how we collect, process, share, and protect Personal Data. It also explains the rights you may have in relation to your Personal Data and how you can exercise them.

Kaltura is a global company with offices in various jurisdictions. We are committed to processing your Personal Data in accordance with fair information practices and applicable Data Protection Laws. While this Candidates Privacy Notice is intended to describe the broadest range of our data practices globally, those practices may be more limited in some jurisdictions based on the applicable Data Protection Law. For example, the laws of a particular country may limit the types of Personal Data we can collect or the way we may process that data and retain it, where in other territories we will be required to retain Personal Data for longer periods. In such cases, we adjust our internal policies and practices to reflect applicable local requirements. This Candidates Privacy Notice further includes or incorporates specific information required under applicable Data Protection Laws for residents of certain jurisdictions, among others:

- **Israeli Candidates** - You are not legally required to provide Personal Data to Kaltura. Providing Personal Data is voluntary and based on your free will and consent. However, if you do not provide certain Personal Data, we may be unable to fulfill specific purposes. For example, we may need certain Personal Data to confirm that you have the required certifications or qualifications for a position, or to comply with legal obligations (such as verifying your right to work in Israel). Accordingly, certain types of Personal Data are necessary for us to evaluate your application. Some other types of Personal Data shall be subject to your choice whether to share with us or not. All purposes are as described under Section 2 below "THE TYPES OF PERSONAL DATA WE PROCESS AND PURPOSE OF PROCESSING".
- **EEA or UK Candidates** - This Candidates Privacy Notice further describes our lawful bases for processing Personal Data, cross-border data transfers, how to contact our DPO or DPR (as described below), and additional information we are required to provide under the EU/UK General Data Protection Regulation ("**GDPR**"), including your rights in relation to your Personal Data under the GDPR.
- **California Candidates** - This Candidates Privacy Notice further describes the categories of Personal Information we collect, and additional information regarding our privacy practices as required under the California Privacy Rights Act ("**CCPA**"), including your rights under the CCPA.

[1] Kaltura Group shall mean either one of the following, as applicable: Kaltura, Inc.; Kaltura Ltd.; Kaltura Europe Ltd.; Kaltura Germany GmbH; Kaltura Asia Pte. Ltd.; Kaltura Portugal Unipessoal LDA.

If you have any questions or concerns regarding our processing of your Personal Data, please contact our Data Protection Officer at: DPO@kaltura.com. If you submit your application through our website, the website's privacy policy will also apply and will govern the collection of data relating to your access to and use of the website.

1) DATA CONTROLLER INFORMATION

Under applicable Data Protection Laws, Kaltura Ltd. and the relevant Kaltura affiliate or subsidiary that offers the position you applied for are the "***data controller***" (or the "***business***" under the CCPA) of your Personal Data. This means that they determine how and why your Personal Data is used and stored (as described in this Candidates Privacy Notice) and how you may exercise your applicable rights.

- If you have any questions or concerns about this Candidates Privacy Notice or our processing of your Personal Data, please contact our Data Protection Officer at: *DPO@kaltura.com*.
- EEA or UK Candidates may also contact our EU GDPR Representative: Kaltura Germany GmbH (Kaltura's Germany-based subsidiary) at:

  Kaltura Germany GmbH c/o Mazars Tax GmbH Theodor-Stern-Kai 1 60596 Frankfurt

  Phone: +1 800 871 5224

2) THE TYPES OF PERSONAL DATA WE COLLECT AND THE PURPOSE

"**Personal Data**" or "**Personal Information**" refers to information that identifies, relates to, or could reasonably be linked with an individual by reasonable means. For example, it could include your name, email address, and other contact information (address, telephone number), etc. Personal Data may further include types of information defined under applicable Data Protection Laws as "**Sensitive Data**" under applicable Data Protection Laws (also defined as "*Highly Sensitive Information*", "*Special Categories of Personal Data*" and "*Sensitive Personal Information*" or the equivalent under applicable Data Protection Laws) which may include information such as governmental identification number or certificate, information that reveals racial or ethnic origin, religion, health related information, etc.

We may collect, store, use, and otherwise process various categories of Personal Data about Candidates, which may include Sensitive Data. These categories are described in the table below. The specific categories or types of Personal Data collected may vary depending on the position and legal requirements in the applicable jurisdiction.

The table below sets out the categories of Personal Data that we may collect:

TYPES OF PERSONAL DATA THAT MAY BE COLLECTED (DEPENDING ON APPLICABLE LAWS)	PURPOSE OF COLLECTION AND USE	CATEGORIES UNDER THE CCPA[2]	LAWFUL BASES (APPLICABLE FOR CANDIDATES LOCATED IN THE EEA OR UK*[3])
▪ **Personal identification information:** such as name, date of birth, government-issued identification number, and copy of identification certificate (e.g., ID, passport, SSN). ▪ **Contact information**: such as email address, phone number, and address. ▪ **Employment history**: such as previous employers, job titles, dates of employment, responsibilities, achievements, etc. ▪ **Education and qualifications:** such as information on educational institutions attendance and dates, degrees or certifications obtained, fields of study, etc.	▪ **Job Application evaluation**: to assess the Candidate's experience, qualifications, skills, and suitability for the position applied for, and in addition, subject to applicable Data Protection Laws, to identify potential matches with other open positions offered by us. ▪ **Communication with the Candidate**: to facilitate our correspondence and communications with the Candidate during the recruitment process, including scheduling interviews, providing updates, and addressing inquiries. ▪ **Verification and reference checks:** to verify the accuracy of the information provided by the Candidate, including employment history, education, and professional references, as well as conducting background checks where necessary and subject to applicable laws.	**Category A** – Identifiers. **Category B** – Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). **Category G** – Geolocation data. **Category I** – Professional or employment-related information. **Category J** – Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99)	The lawful bases depend on the purpose for which we collect, use, and retain Personal Data. We mainly collect and use the Personal Data under our legitimate interest, as needed to decide if to appoint a Candidate to a certain job position. We may further retain certain types of Personal Data, under our legitimate interest, for the purpose of record keeping, compliance with applicable laws, evaluating our recruiting processes, and addressing potential disputes or legal claims. In addition, we retain Personal Data where we are required to do so in order to comply with our legal obligations. Where required under applicable Data Protection Laws, we will obtain your consent in order to retain and further use Personal

[2] This table also represents the categories of Personal Data, as classified and required under the CCPA which has been collected by Kaltura in the preceding 12 months.

[3*] Where the EU or UK General Data Protection Regulations apply, and as required under these regulations.

▪ **Skills, capabilities, and expertise:** such as information related to the Candidate's relevant competencies, skills, language proficiency, and any other expertise that may be pertinent to the position being applied for. ▪ **Assessment results:** information gathered from tests, interviews, or assessments conducted during the recruitment process to evaluate the Candidate's suitability for the role. ▪ **Background check information**: information obtained through background checks , such as verification of employment and education history, and where applicable subject to law's requirements or restrictions, information about criminal convictions and offences. ▪ **Eligibility to work:** information regarding the Candidate's legal right to work in the relevant country, such as citizenship or visa status.	▪ **Compliance with legal requirements:** to ensure adherence to relevant employment laws, regulations, and industry standards. ▪ **Eligibility to work:** to confirm the Candidate's legal right to work in the relevant country and comply with immigration requirements, if applicable. ▪ **Decision-making and selection:** to facilitate the decision-making process, compare Candidates, and ultimately select the most suitable individual for the position. ▪ **Record-keeping and documentation:** to maintain a record of the recruitment process, including Candidate evaluations, assessments, and decisions, which may be used for future reference or to address potential disputes or legal claims. ▪ **Administration and performance of human resources related duties, obligations, and procedures**. ▪ **Continuous improvement**: to analyze and refine our recruitment strategies, practices, and processes.		Data for future job opportunities. You have the right to withdraw consent at any time.

▪ **Communication and internal records:** such as correspondence, and records or recordings of phone/video calls or other interactions between the Candidate and us during the recruitment process. ▪ **Any additional information voluntarily included by the Candidate in its resume (CV), and supporting documents submitted by the Candidate**.			
▪ **Sensitive Data:** we may collect certain information that, depending on the applicable Data Protection Law, might be considered as Sensitive Data. Sensitive Data will be collected solely where there is a specific law requirement or necessity to obtain it, or in the event provided **voluntarily** by the Candidate or otherwise where the Candidate provided its consent. Such information may include Personal Data on about the privacy of a Candidate's family life or personality, a personality assessment	▪ **Record-keeping and documentation:** to maintain a record of the recruitment process, which may be used for internal and external reporting responsibilities (e.g., legal and regulatory requirements), future reference or to address potential disputes or legal claims. ▪ **Equal opportunity monitoring:** we may ask for such information for the purpose of monitoring **equal** opportunity and ensuring diversity and inclusion. ▪ **To ensure compliance with applicable laws or security standards:** to the extent required or permitted by applicable law, we may conduct background checks that may involve criminal record information.	**Category B** – Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). **Category C** – Protected classification characteristics under California or federal law. **Category L** – Sensitive personal information.	We collect these types of Personal Data subject to your consent. You have the right to withdraw consent at any time. We may further retain certain types of Personal Data, under our legitimate interest, for the purpose of record keeping, compliance with applicable laws, evaluating our recruiting processes, and addressing potential disputes or legal claims.

(conducted by a professional entity to evaluate significant personality characteristics) race, ethnicity, national origin, disability and medical or health condition, veteran or military status, or other protected characteristics, and certain data that might be gathered as part of background checks (such as criminal records, as set forth above).	▪ **Administration and performance of human resources related duties, obligations, and procedures.** Note that, we do **not** discriminate, either directly or indirectly, on the grounds of sex, sexual orientation, gender, ethnic origin, religion, belief, marital status, nationality, national origin, color, age, or similar protected characteristics.		

3) CATEGORIES OF SOURCES OF PERSONAL DATA

We typically collect Personal Data about Candidates, as follows:

- **Provided directly by the Candidate** – this includes information you provide when submitting your application and/or at other stages of the recruitment process, such as your name, email address, mailing address, telephone number, age, education history, and similar details; and
- **Provided by third parties** – for example, recruitment agencies, providers of criminal background checks, your references and/or former employers, and other relevant third parties; and
- **Derived from publicly available sources** – for example news sources/social media platforms.

4) WITH WHOM WE SHARE YOUR PERSONAL DATA

We may share your Personal Data with third parties, including within Kaltura, as well as with contractors, consultants, and service providers that support our recruitment activities and our operations, and assist with the administration and performance of human resources-related duties, obligations, and procedures. We may also share your Personal Data where necessary to comply with applicable legal obligations, or to exercise or defend our rights. We implement appropriate measures to help ensure that your Personal Data is accessed only by individuals who have a legitimate need to know it in order to perform their roles, and by third parties that require such access to provide services to us, in accordance with our instructions.

Additional details regarding the categories of these third-party recipients are provided below.

CATEGORY OF RECIPIENT	CATEGORY OF PERSONAL DATA	PURPOSE OF SHARING
Kaltura	All types of Personal Data (Category A, B, C, G, I, J, L under the CCPA)	We may share Personal Data within our affiliated companies and subsidiaries to administer and manage our recruitment process at an organizational level and for broader human resources management purposes. In addition, if a third-party transaction occurs - including a merger, acquisition, insolvency or bankruptcy proceeding, or a sale or purchase of all or a portion of assets - your Personal Data may be disclosed to the parties involved in connection with, and as necessary to effect, such transaction.
Contractors and service providers	All types of Personal Data (Category A, B, C, G, I, J, L under the CCPA)	We may share Personal Data with our trusted agents, contractors, and service providers (for example, human resources agencies, recruitment management SaaS providers, cloud providers, and legal counsel). We share your Personal Data with these third parties so they can provide services to us and support our recruitment and related operations. These parties are restricted from using your Personal Data for any purpose other than performing services on our behalf in accordance with our instructions, or as required to comply with applicable law.
Governmental agencies, or authorized third parties	Subject to law enforcement or a competent authority request.	In the event of legal and law enforcement, we may disclose certain Personal Data, such as in response to verified requests relating to criminal investigations or alleged illegal activity, or any activity that may expose us, you, or any other third party to legal liability, and solely to the extent necessary to comply with such purpose.

We may also share Personal Data where and to the extent necessary to: (a) protect you or others; (b) enforce our policies and agreements or defend our rights, including investigating suspected violations, alleged unlawful activity, or suspected fraud or security incidents; and (c) respond to or participate in disputes, claims, demands, or legal proceedings involving you and us (or a third party), where required to protect our legitimate interests and as permitted by applicable law. We may also disclose Personal Data to third parties if you ask us to do so. In such cases, any Personal Data you choose to share will be subject solely to the relevant third party's own policies and practices.

We do not “sell” your Personal Data to any third party, nor do we “share” it as those terms are defined under the CCPA, meaning we do not disclose or make available your personal information in exchange for money or other valuable consideration. In addition, we do not process your Personal Data for automated decision-making (meaning, where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

5) INFORMATION SECURITY & CROSS BORDER DATA TRANSFER

We take the security of your Personal Data seriously. We use industry-standard procedures and policies designed to protect your Personal Data and to prevent unauthorized access, use, or disclosure. Access to your Personal Data is restricted to employees, agents, contractors, and other third parties who have a legitimate "need to know" and who may process such data only in accordance with our instructions. We also maintain technical, physical, and administrative safeguards to protect the Personal Data we collect and store, including measures intended to identify, address, and manage suspected or actual security incidents.

While we take reasonable measures to protect Personal Data, we cannot guarantee that unauthorized access will never occur, and we are not responsible for the actions of individuals who obtain unauthorized access to or misuse our systems or networks. Subject to applicable Data Protection Laws, we will notify you and the appropriate authorities if we become aware of a security incident or breach involving your Personal Data.

Due to our global operations, your Personal Data may be processed or accessed in provinces, states, territories, or countries outside your jurisdiction, including where it is accessed by our personnel, service providers, or affiliates. This may include transfers of Personal Data to, from, or within Israel, the United States, or the EEA. We only transfer Personal Data to another country in accordance with applicable Data Protection Laws. We take appropriate measures to ensure that your Personal Data receives an adequate level of protection, including by using contractual obligations or other data transfer mechanisms that were pre-approved by applicable data protection authorities to ensure your Personal Data is protected.

6) DATA RETENTION

In general, we retain your Personal Data only for as long as reasonably necessary to fulfill the purposes for which it was collected, including to meet any applicable legal, administrative, recordkeeping, or reporting requirements.

The criteria we use to determine applicable retention periods include the following:

- **The type of Personal Data and purpose of the collection** – we consider the scope, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process your Personal Data, and whether those purposes can be achieved through other means. If and when we no longer have a legal basis to retain Personal Data, we will delete it or de-identify it so that it can no longer be reasonably associated with you.
- **Compliance with our legal obligations** – we may be required to retain certain types of Personal Data to comply with obligations under applicable law. We may also retain Personal Data where required under a binding legal request or a court order.
- **Disputes, claims, and legal proceedings** - if you have a dispute with us, we may retain certain Personal Data as necessary in connection with your claim(s), including throughout any legal proceedings between you and us and, where appropriate, after resolution of the dispute in accordance with applicable statutory limitation periods. In addition, **if** you request to exercise your rights, we will retain relevant correspondence for as long as necessary to demonstrate compliance, typically in line with applicable statutory limitation periods.

We may further retain your Personal Data where you were not hired, to allow us to reconsider your application for alternative or future positions, and where required under applicable Data Protection Laws, we will obtain your consent. In addition, we may retain limited Personal Data as a reference for any future applications submitted.

7) YOUR RIGHTS REGARDING YOUR PERSONAL DATA AND HOW TO EXERCISE THEM

We respect your privacy and your rights to control your Personal Data. You have the right to control and request certain limitations or rights to be executed with regard to the Personal Data we hold and process. Depending on the territory and the applicable Data Protection Laws, and any relevant exceptions, these rights may include one or more of the following:

- **The right to be informed/right to know** what Personal Data we collect about you, the purposes for collecting it, with whom we share it, and other information (including the categories of sources from which we collect Personal Data) as described in this Candidates Privacy Notice;
- **The right to request access to/inspect your Personal Data**, which entitles you to review or receive a copy of certain Personal Data we hold about you;
- **The right to correct ("rectify") inaccuracies in your Personal Data,** which entitles you to have incomplete or inaccurate Personal Data corrected (or, where applicable, to request deletion of inaccurate information);
- **The right to request deletion**, which entitles you to ask us to delete certain Personal Data, subject to applicable Data Protection Laws that may permit or require us to retain some information in specific circumstances;
- **The right to request restriction of processing of Personal Data,** which entitles you to ask us to limit the purposes for which we process your Personal Data (subject to the conditions and exceptions under applicable Data Protection Laws);
- **The right to object,** which entitles you to object to our processing of your Personal Data (subject to conditions and exceptions under applicable Data Protection Laws);
- **The right to data portability**, which entitles you to receive certain Personal Data you have provided to us in a structured, commonly used, and machine-readable format and, where supported, to transmit it to another party;
- **The right to withdraw consent**, where our processing of your Personal Data is based on your consent;
- **The right to be informed of automated decision-making**, which entitles you to receive information about instances in which your Personal Data is used to make a decision based solely on an automated process, where required by applicable law;
- **The right to limit the use and disclosure of Sensitive Data** by Kaltura, where applicable;
- Exercise your privacy rights **without receiving discriminatory treatment** by us; and/or
- **The right to appeal or lodge a complaint**. If we decline to take action on your request, we will notify you without undue delay, as required under applicable Data Protection Laws. Our response will include the reason(s) for the decision and, where required, information on how you may appeal or

submit a complaint to an applicable authority. For EEA/UK Candidates, you may lodge a complaint with the relevant Data Protection Authority in the EU or with the Information Commissioner in the UK.

The rights described above are not absolute and may be subject to legal, business, or contractual requirements. Applicable Data Protection Laws may allow or require us to deny your request, in whole or in part.

You may exercise your rights in relation to your Personal Data by contacting us in writing at DPO@kaltura.com.

If you are a resident of the EU or the UK, you may also submit a request to our EU GDPR Representative using the contact details provided in Section 1 of this Candidates Privacy Notice.

We may need to request specific information from you to help verify your identity and confirm that the requested rights apply to you. This is a security measure to help ensure that Personal Data is not disclosed to anyone who is not entitled to receive it. Information provided in connection with such a request will be used only to process and respond to your request and may be shared with our legal and administrative teams for that purpose.

8) AMENDMENTS

We reserve the right to update this Candidates Privacy Notice from time to time. Any revised version will take effect upon posting. We encourage you to review this Candidates Privacy Notice periodically to stay informed about our privacy practices and any changes.

If we make material changes, we will provide a more prominent notice and/or obtain consent where required by applicable law.