

# Candidate Privacy Notice

Rev. Mar 19, 2024

This Candidate Privacy Notice (“Notice”) applies to personal information Conviva Inc., including any of its affiliates (collectively “Conviva,” “we” or “us”), collects about its job applicants and how it handles such information during the application process.

For the purposes of this Notice, “Personal information” is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a job applicant. This may include your name, email address, location, job title and company or employer, your user ID and password when you apply, IP address, and other information described in this Notice. The country in which the position is located will determine the types of personal information we receive. Should you apply to more than one location, or should the role be available in more than one country, the personal data processed are determined by each of those countries where the position is located.

Personal information does not include anonymized, de-identified, or aggregated information which does not personally identify you.

You are being provided this Notice because you are applying for work with us (whether as an employee or contractor). When you sign-up for job alerts or apply to a job posting directly with Conviva, the personal information contained in your application will be collected by Conviva’s third party provider(s) and shared with us.

This Notice does not apply to data about our employees, contractors, clients, or other personal information that Conviva collects for other purposes. Please review our [Privacy Policy](#) to learn how information provided through our website and/or services is processed.

## Types of Information Collected

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you. We do not collect all of this

information about all candidates, as needs vary by candidate (including depending on their prospective role and the stage of their candidacy), and local recruiting practices and legal requirements vary. Some of this personal data is collected only after an offer is extended.

- ○ **Identifiers:** your name, address, email address, telephone numbers, date of birth, social media profiles/handles, and other contact details including more sensitive data such as your social security number, passport number, driver's license or state ID card number.
- **Internet, electronic network, and device activity and device information and related identifiers:** such as your IP address if you apply for a job through our website.
- **Professional or employment-related Information.**
- **Recruitment, employment, or engagement information** such as application forms and information included in a resume, cover letter, or otherwise provided through the application and recruitment process; information you provide which is required to initiate your employment, such as proof of eligibility to work in a specified country (such as a passport or visa), citizenship or immigration status; references; our evaluations of your performance during the interview process; and if provided an offer, and background screening results (including any criminal convictions).
- **Career information** such as job titles, work history, work dates and work locations, and information about skills, qualifications, and experience.
- **Education information:** institutions attended, degrees, academic record, certifications, licenses, transcript information, and professional memberships.
- **Business travel and expense information:** travel itinerary information and expenses incurred for travel during the interview process.
- **Audio or visual information** such as CCTV footage, as well as other information relating to the security of our premises collected during in-person interviews or other parts of the recruitment process; and video or audio recordings of the interview process.

- **Potentially protected classification information** to the extent required or as permitted by law and voluntarily provided such as race, sex, gender identity/expression, nationality, ethnicity, citizenship, accommodation information, and other information to help us monitor compliance with equal opportunity legislation.
- **Other information** that you may voluntarily choose to include on your resume or in connection with your application or otherwise.

Sensitive Information: We may also collect, store and use the following types information that may be considered “sensitive personal information” or “special categories of data” under applicable privacy laws:

- ○ Social Security number or passport information for legal compliance and immigration purposes.
- Health information, which may include disability status, to provide reasonable accommodations during recruitment process.
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, if you have provided such information voluntarily through your CV/resume, interview process and/or LinkedIn profile, to ensure meaningful equal opportunity monitoring and reporting.
- Information about criminal convictions and offenses for background check purposes.

## **How is your personal information collected?**

We collect personal information about candidates from the following sources:

- ○ You, the candidate.
- Information provided to our third-party applicant tracking provider.
- Information available from your LinkedIn profile (subject to you explicitly consenting to linking your LinkedIn profile).
- Our external recruitment agencies.
- Our background check provider, from which we collect the following categories of data: criminal record information and education and employment

verification.

- Your named references, from whom we collect the following categories of data: confirming employment and dates of employment.

## **Purpose and Basis for Processing**

We will use the personal information we collect about you for the following business purposes:

- ○ **Administer and process your application**, including verifying your identification, experience and other information you submit and, if your application progresses, any interview information and background check information.
- **Communicate with you about your application**, including contacting you via phone, email or social media platforms about your application and, if your application progresses, any interview and background check information.
- **Assess and evaluate your suitability** for the role for which you have applied, or for other vacancies, including verifying your identification, experience and other information you submit and, if your application progresses, any interview information and background check information.
- **Conduct reference and background checks** as part of your application, subject to applicable law, including verifying your identification and other information you submit and, if your application progresses, we will conduct background checks on your criminal history and verify your education and employment history.
- **Comply with applicable laws and employment-related requirements**, including verifying identification information and information required to initiate employment, for purposes such as confirming ability to legally work in a specific location, complying with statutory reporting requirements, and responding to and cooperating with legal or regulatory requests and investigations.
- **Exercise our legal rights**, including seeking legal advice from our external lawyers or in connection with litigation with a third party.

- **Inform you of career opportunities**, including other vacancies for which you may be eligible.
- **At your request**, in order to fulfill your instructions.

We may also use personal information for any other legally permitted purpose (subject to your consent, where legally required).

We will normally only collect and process your information where:

- ○ we need to comply with legal obligations applicable to us (such as applicable immigration and/or employment laws and regulations);
- we need the information to fulfill our responsibilities in any actual or prospective agreement with you (such as an employment agreement or an offer of employment, if you are considered for employment);
- the processing is necessary for our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms (such as to ensure a safe working environment for all our staff, and to ensure the reliability of our candidates, and otherwise to administer and process your application, or to communicate with you about your application); or
- we have your consent to do so.

Where we collect and process special categories of data (for example, race, gender), then we will only process such information:

- ○ where we reasonably need to do so in order to comply with our legal obligations as a prospective employer;
- where we need to do so in order to assess your working capacity;
- where we need to do so to protect your or another person's vital interests (and we are unable to obtain your consent); or
- where you have given us your consent.

Certain information we collect may be considered "**Sensitive Personal Information**" under the California Consumer Privacy Act ("CCPA"). We collect and process such information only for our legitimate business purposes and do not process such information for purposes for which the "right to limit" applies under the CCPA.

California law also places certain obligations on businesses that “sell” personal information to third parties or “share” personal information with third parties for “cross-context behavioral advertising” as those terms are defined under the CCPA. We do not “sell” or “share” the personal information covered by this Notice and have not done so in the twelve months prior to the effective date of this Notice.

## **What happens if you do not provide personal information?**

If you fail to provide information which is necessary for us to consider your application (such as evidence of qualifications or work history) when requested, we will not be able to process your application successfully. For example, if we require a background check or references for the role you apply for and you fail to provide us with relevant details, we will not be able to take your application further.

## **Background Checks**

If we extend an offer to you and you agree to continue the application process, we will perform a background check in compliance with applicable local law and collect information about your criminal conviction history and verification of your prior education and employment history. We require background checks in order to confirm that there is nothing in your criminal convictions history which makes you unsuitable for the role and that your education and employment history is consistent with what we have in your application file. Any employment offer is conditional upon a successful background clearance check.

## **How We Disclose Personal Information**

We may disclose certain personal information to the following types of entities or in the following circumstances (where applicable):

- ○ **Internally:** to employees within Conviva that participate in the recruitment process, such as HR managers and employee interviewers.
- ○ **Vendors:** such as background check companies, security providers, information technology providers, travel management companies, and

employment businesses (e.g., recruiting contractors or agency workers) that provide us with services relevant to recruiting and hiring.

- **Recruiters:** to the extent you are working with a recruiter in connection with your application for employment and your recruiter is authorized by you to obtain feedback from us regarding your application and interview process.
- **Legal compliance and exercising legal rights:** (i) when required to do so by law, regulation, or court order, (ii) in response to a request for assistance by the police or other law enforcement agency, (iii) to seek legal advice from our external lawyers or in connection with litigation with you or a third party, or (iv) as otherwise necessary to exercising our legal rights or to protect the Company or its employees.
- **Business transaction purposes:** in connection with the sale, purchase, or merger of all or a portion of our Company.
- **Consent:** with your consent and as permitted by law, we may disclose personal information to any other parties in any other circumstances.

## **Data Transfer Abroad**

We operate internationally and, as a result, if such data does not originate from within the United States, we will transfer candidate information across international borders, including from the European Economic Area (EEA) to the United States, for processing and storage. To the extent that your data is transferred outside the EEA, we will transfer such data consistent with applicable data protection laws.

## **Data Security**

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know.

## **Data Retention**

The personal information we collect from job candidates will be retained until we determine it is no longer necessary to satisfy the purposes for which it was collected and our legal obligations. As described above, these purposes include our business operations and complying with reporting, legal and accounting obligations. In determining how long to retain information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorised use or disclosure of the personal information, the purposes for which we process the personal information and whether we can achieve those purposes in other ways, the applicable legal requirements, and our legitimate interests.

Where personal information is kept beyond the time that we normally would need to keep it, that period will be determined based on the applicable local law. Because we may collect and use the same category of personal information for different purposes and in different contexts, and because rules differ by jurisdiction, there is not typically a fixed retention period that always will apply to a particular category of personal information.

To provide security and business continuity for the activities described in this Notice, we make backups of certain data, which we may retain for longer than the original data.

## Your Data Rights

To the extent provided for by law and subject to applicable exceptions, you may have the following rights in relation to the personal information we collect:

- ○ **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to

processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.
- **Withdraw your consent to our collection and processing** of your information at any time.
- **Request deletion or removal** of certain of your personal information.
- **Lodge a complaint** at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues arising from job applicant data processed in the EEA.

You also have the right not to be discriminated against (as provided for in California law) for exercising your rights.

If you wish to exercise any of these rights, please contact [privacy@conviva.ai](mailto:privacy@conviva.ai), [submit a form](#), or contact us at 1-888-203-0378. We may request proof of identification to verify your request.

If you are an agent making a request on behalf of a candidate, we reserve the right to take steps to verify that you are authorized to make that request, which may include requiring you to provide us with written proof such as a notarized authentication letter or a legally sufficient power of attorney signed by the data subject pursuant to California Probate Code sections 4121 to 4130, or other written authorization acceptable to us. We also may require the candidate to verify their identity directly with us where permitted.

We are not responsible for the security risks of this or any other arrangements that a candidate may have with an agent. For clarity, this is not permission for any applicant to disclose their login credentials to an agent or any third party. Such disclosure is

prohibited and is not required for an agent to make requests under this Notice.

For security and legal reasons, however, Conviva reserves the right not to accept requests that require us to access third-party websites or services.

## **Further Information**

If you require clarification regarding this Notice, or need to access it in an alternative format, please contact [privacy@conviva.ai](mailto:privacy@conviva.ai). If you are a job candidate in the EEA, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.