This Applicant Privacy Policy, hereby referred to as the “Policy,” describes the privacy practices that apply to Camunda Services GmbH and its subsidiaries’, hereby referred to as “Camunda,” “we,” “us” and “our”; collection, use and disclosure of information relating to how an identified or identifiable applicant, hereby referred to as the “Applicant” engage with Camunda for employment or internship opportunities, via any method, as well as how Camunda uses and shares that information.

Contact Camunda

Camunda Services GmbH is Controller within the meaning of the GDPR and of other data protection laws or provisions applicable in the Member States of the European Union.

If you have any questions or concerns regarding this Policy please contact Camunda via our webform or by postal mail to:

Camunda Services GmbH

Zossener Strasse 55-58

10961 Berlin Germany

Or phone: +49 30 664 04 09 – 00

Camunda has appointed a Group Data Protection Officer.

The Data Protection Officer for Camunda is:

Farrhah Khan

For questions about how information is gathered, stored, shared, used, or to exercise any data subject rights, please contact our Data Protection Officer as follows:

E-mail: privacy@camunda.com

Personal Data Camunda Collects

In order to process applications, Camunda asks the Applicant to provide Personal Data. This information is provided voluntarily, and the Applicant determines the amount and type of information provided; however, some information may be necessary to complete an evaluation of the application and for the Applicant to be considered as a candidate.

The Applicant usually provides Camunda with personal data, including educational and employment background, contact information, work permit or visa information, and other career opportunities for which the Applicant would like to submit to. This personal data may come in the form of a CV, resume, cover letter, educational transcripts, and employment references. In addition, the following data may be collected: audio and/or video recordings of interviews, AI-generated transcripts and summaries of interview conversations, and interviewer notes as well as metadata related to the interview such as date, time, and duration.

Camunda does not require any information from the Applicant that the German General Equal Treatment Act (AGG) prohibits or information that would qualify as sensitive personal data under GDPR, including information relating to race, ethnicity, gender, religion

or world-views, disability, age or sexual orientation. Information about illnesses, pregnancy, political views, philosophical or religious convictions, membership of a trade union, physical or mental health or sexual preferences are similarly not to be transferred.

How Camunda Uses Personal Data

Camunda uses Applicant Personal Data (as set out above) in the application and recruitment process for purposes including:

- Assessing qualifications, skills, and interests against current Camunda career opportunities;
- Verifying the information the Applicant provides and completing reference checks;
- Facilitating the recruitment and interview process, including communicating with you with regards to your application;
- Recording and summarizing interviews to support accurate and consistent evaluation of candidates by the hiring team;
- Preparing an offer letter, if applicable;
- Complying with applicable laws, regulations, legal processes or enforceable governmental requests, including protecting the rights and property of Camunda, Camunda users, applicants, candidates, employees or the public;
- Producing reports related to recruitment metrics;
- Managing and improving Camunda's recruitment processes;
- Fraud Prevention - To protect the integrity of our recruitment process, Camunda also uses Applicant Personal Data for fraud detection and prevention. We utilize an automated feature provided by our service provider, Ashby, Inc., to analyze certain technical data associated with your application, including your device information, IP address, email address, and phone number. This process helps us identify and flag applications that may be fraudulent. This fraud detection process assists our recruitment team but does not constitute a solely automated decision under Article 22 of the GDPR. All flagged applications are subject to manual review by a human recruiter before any decision is made regarding your candidacy.

Application data of promising candidates may be kept, for those who opted into the Camunda TalentPool, in order to notify the Applicant of a suitable position.

Information collected during the application and recruitment process will become part of the Applicant's employment record, if offered and accepted employment with Camunda.

We do not sell or share personal information for marketing purposes with third parties.

How Camunda Shares Personal Data

Camunda limits access to the Applicant's Personal Data to only those who need access to perform recruitment tasks and duties, and to third parties who have a legitimate purpose for accessing it such as in the following circumstances:

- Service providers: Applicant Personal Data may be shared with service providers, agents or other third parties, e.g., recruiters, consultants, and attorneys, when the Applicant applies via Camunda's online applicant platform, and the data is transferred directly to Camunda's third party provider, Ashby, Inc.. In addition, Camunda uses BrightHire, Inc. as a service provider to record and process interviews. Interview recordings and AI-generated summaries may be shared with BrightHire, Inc. for this purpose. Camunda requires third parties to protect the information they receive and prohibits them from using the information for their own purposes.

- Compliance with laws, regulatory bodies, or government agencies: Camunda may disclose Applicant information when disclosure is necessary or required by law or regulation, to comply with legal process or government requests, or to exercise, establish or defend our legal rights.
- With Applicant consent: Camunda may disclose Personal Data for any purpose with the Applicant's consent.

Legal Basis for Processing Applicant Personal Data

Camunda's legal bases for processing Applicant Personal Data include:

The purpose of the data processing is to support the decision on whether an applicant is suitable for a post at Camunda and whether a contract of employment can be entered into with them.

- The legal base to keep data in the talent pool is Art. 6 I a GDPR.
- The legal basis for processing the data after the user has submitted the application is Art. 88 GDPR in conjunction with section 26 of the Federal Data Protection Act (BDSG).
- Consistent with specific Applicant consents (e.g. for Camunda's TalentPool), which the Applicant may revoke at any time in accord with Art. 6 I a GDPR.
- As necessary to comply with Camunda's legal obligations in accord with Art. 6 I c GDPR.
- To protect the Applicant's interests or the interests of others in accord with Art. 6 I d GDPR.
- The forwarding of application data to Ashby, Inc. is similarly justified pursuant to Art. 28 GDPR and Art. 6 I f GDPR. As necessary for Camunda's legitimate interests in considering candidates for current and future employment opportunities in accord with Art. 6 I f GDPR.
- The processing of interview recordings and summaries is based on the Applicant's consent in accord with Art. 6 I a GDPR, obtained prior to each interview. Where the Applicant opts out, no recording or AI processing will take place. The forwarding of data to BrightHire, Inc. is further justified pursuant to Art. 28 GDPR and Art. 6 I f GDPR as necessary for Camunda's legitimate interests in conducting a fair and consistent interview process.
- For transferring and storing personal data in the US, Camunda will collect a user's consent in accord with Art. 49 I a GDPR.

Retention of Applicant's Personal Data

Camunda retains Applicant Personal Data for as long as required to comply with legal obligations, resolve disputes, and to enforce our contractual agreements or as necessary for our legitimate interests.

If the Applicant is successful in their application for a position at Camunda, we retain the information that is provided during the application process, and information about the application process, as part of the Applicant's employee records.

If the applicant is not offered employment, all application data will be automatically deleted six months after notifying them that their application was unsuccessful, unless the Applicant requests to be in Camunda's TalentPool to be considered for other roles. Applicant data is stored in Camunda's TalentPool for a period of up to two years.

The Applicant can withdraw the application, the consent to store their personal data or ask to update their data at any time by contacting Camunda via our webform. Further information on data collection, evaluation and processing of the Applicant's data by Ashby, Inc. and on their rights in relation to this can be obtained from Ashby, Inc.'s privacy statement, which is available at https://www.ashbyhq.com/resources/privacy.

International Data Transfers

A user's personal data may be accessed, stored, transferred to and processed in countries other than the country in which the person resides. As an internationally operating company, Camunda may have to access, transfer or process Applicant's Personal Data data in countries outside the European Economic Area ("EEA"), including the USA. These countries may have data protection laws that differ from the laws of the country where the person resides. We have taken adequate security precautions to ensure that such personal data remains protected in accordance with this Policy and we have established adequate mechanisms to protect personal data in agreements with Camunda's service providers such as use the standard contractual clauses of the EU Commission in accordance with Art. 46 II c GDPR.

We work with the application platform provider Ashby, Inc.. When a user applies for a job at Camunda and uploads application data to the platform, Ashby, Inc. stores the users' application data in the US on our behalf. We inform about this and ask for a user's consent for this in accord with Art. 49 I a GDPR. Please also see Ashby, Inc.'s privacy policy and Ashby, Inc.'s Trust Center for more information about Ashby, Inc. and its data protection standards. Ashby, Inc. holds the EU-US, the Swiss-US, and the UK Extention to the EU-US Data Protection Framework Certificates.

Use of AI/ML Features in Application Processes

Camunda may use artificial intelligence (AI) and machine learning (ML) technologies, including natural language processing and predictive analytics, to assist in the initial screening of employment applications. These AI/ML tools assess applications against the characteristics and qualifications relevant to the job requisition. These tools are designed to help identify potentially qualified candidates, and to assist human recruiters. We do not make automated hiring decisions (including per Article 22 of the GDPR). Every hiring decision is closely reviewed and made by a human recruiter.

We take the following steps to ensure fairness, transparency, and data protection:

- Redaction of Personal Identifiers: Before your application is processed by any AI system, personal identifiers such as name, contact details, gender, and photo are removed or anonymized to minimize bias.
- Transparency: Recruiters can see which sections of your application triggered an AI tool suggestion and are instructed to verify or override any AI output.
- No Model Training on Applicant Data: Your personal data is not used to train or improve the AI model.
- Bias Monitoring and Compliance: Ashby, Inc. conducts internal assessments and may engage third parties to evaluate the AI system for compliance with the EU AI Act (Annex III – Employment) and other relevant regulations.

If you prefer not to have your application assessed using AI/ML features, you may opt out by completing the form linked here. After submitting your request, you will receive a confirmation email containing a link to finalize your opt-out. You must click the confirmation link to complete the process. Once your opt-out is confirmed, your application will be reviewed manually by our recruitment team, without the use of AI/ML technologies. Opting out will not negatively impact your application.

Use of BrightHire in the Interview Process

Camunda also uses BrightHire, an AI-powered tool that may record interviews and generate transcripts and summaries of what was discussed. BrightHire serves a purely assistive function — it helps the hiring team capture and review interview content more accurately but is never used to make automated hiring decisions (including per Article 22 of the GDPR). Every hiring decision is closely reviewed and made by a human recruiter.

Prior to any interview where BrightHire is active, the Applicant will receive a separate notice from BrightHire and will have the opportunity to opt out of having the interview recorded and processed by BrightHire's AI features. Applicants may also inform their recruiter at any time if they wish to opt out.

Please note that opting out of Ashby's AI/ML features (via the form above) does not automatically opt the Applicant out of BrightHire. The two opt-out processes are separate.

Opting out of BrightHire will not negatively impact the Applicant's candidacy. Interviews will proceed without recording, and the application will be evaluated in the same manner as any other.

The following safeguards apply to BrightHire:

- No Automated Decision-Making: BrightHire outputs are assistive only and are never used as the sole basis for any hiring decision.
- No Model Training on Applicant Data: Interview recordings and summaries are not used to train or improve BrightHire's AI models.
- Access Restrictions: Access to BrightHire recordings and summaries is limited to members of the hiring team involved in the Applicant's interview process.

Applicant Privacy Rights

The Applicant may have a legal right under applicable law such as the European Union's ("EU") General Data Protection Regulation (GDPR), or the California Consumer Privacy Act of 2018, to access the Personal Data Camunda maintains. Applicants have the right to review, correct, or update Personal Data, or withdraw consent for Camunda to collect any information. Please contact Camunda via our webform to submit a request.

California Privacy Rights

Please see **California Specific Privacy Policy** for information about Privacy Rights of California residents, and other required disclosures.

Applicant Responsibilities

The Applicant is responsible for the information made available to Camunda, and must ensure it is truthful and accurate. In the case information provided concerns another person, such as individuals provided as references, the effected individual must receive notice and give consent in order for Camunda to collect and use that information.

Security

Camunda is committed to protecting the security of Applicant's Personal Data, by using appropriate technical and organizational measures to protect Personal Data from unauthorized access, use, or disclosure, but cannot eliminate security risks and breaches associated with Personal Data. Please contact us with security questions using the instructions in our Trust Center.

Changes to this Policy

Camunda reviews and updates this Policy periodically in response to changing legal, technical, and business developments. Material changes made

to this Policy may require Camunda to inform the Applicant in a manner that is consistent with the significance of the changes made.

Change Log

November 2026: Inclusion of specific statement regarding not selling or sharing personal information for marketing purposes with third parties.

April 2026: This privacy policy has been updated to reflect the use of BrightHire, Inc. as an AI-powered interview recording and summarization tool in the recruitment process.

June 2025: This privacy policy has been revised to reflect the adoption of Ashby, Inc. as the new platform for hosting job applications.

October 2022: This privacy policy has been updated to introduce a new webform to facilitate contacting Camunda around privacy related issues.