

Job Applicant Privacy Policy and Notice at Collection

This Job Applicant Privacy Policy (“**Policy**”) describes how Benchling, Inc. (“**Benchling**”, “**we**”, “**us**” and “**our**”) collects, uses, and discloses information about individuals who apply for open positions at Benchling (“**Benchling Applicants**”).

We may also provide you additional privacy notices regarding our collection, use or disclosure of information from and about you (“**personal information**”). Please read this Policy and any other privacy notices carefully. Please note that this Policy does not form part of any employment contract or contract to provide services.

This Policy does not apply to our handling of data gathered about you in your role as a user of our services. If you interact with us as in that role, the Benchling Privacy Policy applies.

1. Types of Personal Information We Handle

We collect, store, and use various types of information that identifies, relates to, or could reasonably be linked to you (“**personal information**”) in connection with your application for employment with us. We collect such information either directly from you or (where applicable) from another person or entity, such as professional networking websites, job posting websites, employment agencies, recruitment companies, academic institutions, background check providers, or your professional references. We may collect additional personal information throughout the course of your application process.

The information we collect from and about Benchling Applicants includes, where applicable:

- **Identifiers** such as first and last name, postal address, telephone number, and email address, and, if provided an offer, identifiers related to your citizenship documents, such as Social Security Number, national ID card, passport, and copies of work permits and birth certificates (which include date and place of birth).
- **Professional or employment-related information**, including:
 - **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 about your eligibility to work in the country where you are applying for a job, such as information related to citizenship and/or immigration status; references; our evaluations of your performance during the interview process; and if provided an offer, background screening results (including any criminal convictions).
 - **Career information** such as past employers, titles, job history, work dates and work locations, salary expectations, notice period, and information about skills, qualifications, and experience.
- **Education information** such as institutions attended, degrees, academic record, certifications, licenses, transcript information, and professional memberships.
- **Business travel and expense information** such as 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 events and recruitment activities.
- **Internet and electronic network, and device activity and device information and related identifiers**, such as information about your use of our network while you are on our premises, including IP address and device identifiers and attributes.
- **Potentially protected classification information** to the extent required or as permitted by law and voluntarily provided such as race/ethnicity, nationality, sex/gender, gender identity, citizenship, religion, marital status, military service, disability, race, 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, in connection with your application, or otherwise.

2. How We Use Personal Information

We may collect, use, disclose, and store personal information for our business purposes, which include, where applicable:

- **Engaging in the recruitment process**, including communicating with you, interviewing, and selecting and hiring new personnel.
- **HR management and administration**, including determining compensation, scheduling, IT and informational security purposes, fraud prevention, and conducting internal analyses and audits.
- **Security operations**, including detecting security incidents, debugging and repairing errors, and preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution; monitoring and controlling access to our premises and locations (including through use of CCTV); and safeguarding Benchling and its locations, services, and employees.
- **Safeguarding Benchling and the services**, including the protection of Benchling, our workforce, users, partners, and others.
- **Legal compliance**, such as complying with applicable laws, and responding to and cooperating with legal or regulatory requests and investigations.
- **At you request**, in order to fulfil your instructions.
- **Exercising our legal rights**, including seeking legal advice from our external lawyers or in connection with litigation with a third party.

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

Some personal information we collect in the recruitment process, such as ethnicity and veteran status, may be considered “sensitive” under applicable law. We use such information only for equal employment opportunity purposes. Some “sensitive” information may be required for certain job applications.

3. 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 Benchling that participate in the recruitment process, such as HR managers and employee interviewers, and among our corporate affiliates.
- **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 Benchling 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.

4. Data Retention

The personal information we collect from Benchling Applicants 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 unauthorized 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.

Data of Benchling Applicants who do not join Benchling is generally retained for 12 months after the conclusion of the recruitment process so that we can notify you about future roles which may be of interest. You may ask us to delete your records earlier.

5. Additional Information for Residents of California

Residents of California have certain rights regarding their personal information. This section is solely applicable to such residents to the extent that such rights apply. Subject to certain exceptions, if you are a California resident, you may request:

- access to certain of your personal information including the right to know the categories of personal information we have or will collect about you and the reason we will or have collected such information;
- correction of certain of the personal information that we have about you that is inaccurate; or
- deletion or removal of certain of your personal information.

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

Exceptions to Your Rights: There are certain exceptions to these above rights. For instance, we may retain your personal information if it is reasonably necessary for us or our service providers to provide a service that you have requested or to comply with law or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity or prosecute those responsible for that activity.

Exercising Your Rights: To exercise one of the rights above, you may email us at privacy@benchling.com. We will take reasonable steps to verify your identity before responding to a request. In doing so, we may ask you for verification information so that we can match at least two verification points with information we maintain in our files about you. If we are unable to verify you through this method, we shall have the right, but not the obligation, to request additional information from you.

California law 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 California Consumer Privacy Act (“CCPA”). We do not “sell” or “share” the personal information covered by this Policy and have not done so in the twelve months prior to the effective date of this Policy.

6. Additional Information for Residents of Canada

If you are a resident of Canada, subject to the laws of your jurisdiction of residence, you may have certain rights regarding your personal information, such as the right to access or correct certain personal information or the right to decline or object to certain collection, uses, and disclosures of your personal information. For more information and to request to exercise your rights, you may contact us as provided below under “Contact Us.”

7. Additional Information for Residents of the EEA, UK, and Switzerland

This section solely applies to you if you are a resident of the European Economic Area (“EEA”), United Kingdom (“UK”), or Switzerland.

Legal Bases: Our legal bases for processing your personal information as described above in this Policy are:

- **Contract:** We may process your personal information as necessary to perform a contract with you, such as to administer payroll and provide benefits.
- **Legal obligation:** We may process your personal information to comply with a legal obligation or request, such as to comply with employment and tax regulations.
- **Legitimate interest:** We may process your personal information for purposes of our or another party's legitimate interests, such as to maintain the security of our premises, personnel, and property.
- **Consent:** We may process your personal information consistent with your consent to the extent permitted by applicable law.

Your Rights: As provided in applicable law, residents of the EEA, UK, and Switzerland have the right to:

- Access the personal information we process about you, including the right to obtain confirmation of whether we are processing your personal information, access to the personal information we process about you, and a copy of such personal information.
- Request rectification of personal information when you consider that it is inaccurate.
- Erasure of certain personal information in certain circumstances, such as when your personal information is no longer necessary in relation to the purposes for processing or if erasure is necessary for legal compliance.
- Request restriction of certain processing activities, such as when you dispute the accuracy of the personal information.
- Object to certain processing of your personal information.
- Withdraw your consent at any time where we process your personal information based on your consent and not on another legal basis, provided that withdrawing your consent only affects our processing after the withdrawal.
- In some circumstances and if technically feasible, request that your personal information be transferred to a third party or provided to you directly in a structured, commonly used and machine-readable form.
- If provided for under the law of the jurisdiction where you reside, give instructions about the processing of your personal information after your death.

You also have the right to lodge a complaint with your local data protection authority if you believe we have processed your personal information in violation of applicable data protection law. However, we encourage you to raise any complaints with us first so we can do our best to resolve it. A list of EEA data protection authorities is available here: https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-uk. UK residents may find information about the Information Commissioner's Office here: <https://ico.org.uk>. Swiss residents may find information about the Federal Data Protection and Information Commissioner here: <https://www.edoeb.admin.ch/edoeb/en/home.html>.

There are certain exceptions to the above rights. For instance, we may retain your personal information if it is reasonably necessary for us or our service providers to provide a service that you have requested or to comply with law or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity or prosecute those responsible for that activity. In addition, we reserve the right not to process requests that are manifestly unfounded or excessive, as provided in applicable law.

To exercise your rights, please contact us and specify the right(s) you want to exercise and the personal information with respect to which you want to exercise such right(s), as well as

your reasons for wanting to exercise such right(s), if applicable. You can submit your request by emailing our Data Protection Officer at privacy@benchling.com.

International Personal Information Transfers: The personal information that we may provide to our service providers for the purposes of staff administration, the provision of tools necessary for your functions and missions and the management of our premises and information systems are mainly processed and stored on servers based in the EEA, UK, and Switzerland. We also process and store some of your personal information in the United States, where our headquarters are located. If we transfer, or allow our service providers to transfer, some of your personal information to jurisdictions not deemed to be “adequate” by the relevant authorities (i.e., jurisdictions that are deemed not to provide a level of protection to personal information that is equivalent to that of the EEA, UK, or Switzerland), we will transfer such personal information in compliance with applicable law and using a legally recognized transfer mechanism, including the European Commission's Standard Contractual Clauses, and equivalent transfer mechanisms in the UK and Switzerland.

8. Contact Us

If you have questions about our collection, use, or disclosure of personal information, please contact us at privacy@benchling.com.