

Privacy Policy for Job Applicants and Personnel

Welcome to Branch! We are the leading mobile linking platform, with solutions that unify user experience and measurement across different devices, platforms, and channels. This Privacy Policy for Job Applicants and Personnel (the "Policy") describes the information Branch Metrics, Inc. and/or its subsidiaries ("**Branch**", "We", "Us") collect, as well as how we use, retain, share and delete that information as part of our recruiting and employment functions, including for current and former employees, contractors, consultants, interns, and workers.

We may update this Policy at any time. We may also provide you additional privacy notices regarding our collection, use, or disclosure of information. Please read this Policy and any other privacy notices carefully.

This Policy does not form part of any employment contract or contract to provide services. In addition, if you provide services to Branch through or in connection with another company, we are not responsible for that company's privacy practices.

This Policy does not apply to our handling of data gathered about you when you use the services of Branch customers for which Branch technology is integrated. When you interact with us in that role, the privacy policy associated with the relevant Branch customer applies. This Policy also does not apply to our handling of data gathered about you in your role as a user of our services, such as Branch Navigator. When you interact with us in that role, the privacy policy of the relevant service applies.

This Policy will be accessible via our human resource information system and is made available to new employees as part of the onboarding process.

International Data Transfers

Branch is a United States company. By performing services for Branch as an employee, contractor, consultant, intern, or worker, you agree that your information will be transferred to and stored within the United States. If you are located outside of the United States, please note that applicable data protection laws may not be equivalent to the laws of your local jurisdiction. Branch implements safeguards necessary to comply with the GDPR and other applicable privacy laws.

Information We Collect

This policy covers the information we collect during the application and recruiting process. This data, which may be collected directly from you or third parties, includes:

- Identifiers, such as your name, email address, phone number, and other information about you, and such information about your beneficiaries or emergency contacts;
 - Your resume or CV, cover letter, copies of identification documents, such as driver's licenses, passports, visas, background reports, and any other personal information you submit as part of your employment application;
 - Career information such as work experience, job titles, work dates and work locations, performance information, information about skills, qualifications, experience, publications, and speaking engagements; absence and leave records; professional memberships; disciplinary and grievance information; and termination information;
 - Financial information, such as information that may be necessary for the administration of payroll, and bank account and tax information;
 - Business travel and expense information, such as travel itinerary information, corporate expenses, and Branch credit card usage;
- Education information, such as institutions attended, degrees, certifications, training courses, publications, and transcript information;

- Legally protected classification information, such as sensitive information you submit as part of the application or recruitment process, including demographic information, health information, religious beliefs, sexual orientation, marital status, nationality, and ethnicity;
- Sensitive personal information, such as Social Security Number, passport number, and driver's license number. Some other information, such as legally protected classification information, may be considered "sensitive personal information" under California law;
- Electronic and other workplace monitoring information. We may monitor your activity (including online activity) on Branch networks or Branch-issued technology (e.g., smartphones, laptops, tablets, etc.);
- Internet, electronic network, and device activity and device information and related identifiers such as information about your use of the Branch network, information, and communication systems, including user IDs, passwords, IP addresses, device IDs, web logs, metadata, and audit trails of system access;
- Audio or visual information, such as CCTV footage, as well as other information relating to the security of our premises; recorded presentations in which you participate; and photographs taken at Branch functions;
- Medical information about you, and, if applicable, your beneficiaries, such as dependent information, spousal or partner information, health information, sickness records, and medical conditions;
- Other information that directly or indirectly identifies you, such as date and place of birth, citizenship, and permanent residence (and such information about your dependents or emergency contacts); and information on any publicly available social media profile of yours that mentions your connection to us or our services.

How We Use Your Information

Branch collects personal information about you to carry out the application and recruitment process, and to support day-to-day business and human resources functions and activities, including:

- For talent acquisition and employee lifecycle management purposes, such as recruiting and hiring job applicants (including, where permitted by and in compliance with applicable law, conducting background checks), administering employee compensation and benefits, soliciting survey feedback to improve the employee experience, and managing the employee termination process;
- For performance management purposes, including performance reviews, employee mobility and talent development, and attendance monitoring;
- For operational purposes, such as for processing payroll, administering benefits, managing the company directory, accounting for purchases by employees, managing workplace safety and security, managing Branch's network and systems, and developing business continuity and disaster recovery plans;
- For policy enforcement purposes, such as conducting ethics and disciplinary investigations, administering and enforcing privacy and security training programs, and managing audit and compliance matters;
- To comply with applicable laws, regulations, legal processes, or enforceable government requests as necessary; and
- To exercise our legal rights, including seeking advice from our external lawyers or in connection with litigation with a third party.

Certain information we collect may be "sensitive personal information" under California law. We use such information as legally necessary to conduct our relationship with you, in the following ways:

- Social Security Number or government identifiers such as passport number, driver's license number, or state ID card number for legal compliance, payroll, benefits, tax, and immigration purposes;
- Health information, which may include disability status, to provide reasonable workplace accommodations and manage absences, for workplace health and safety purposes, and for compliance with applicable law and contracts or to exercise rights thereunder;

- Racial/ethnic origin, sexual orientation, and/or disability status for equal opportunity and diversity and inclusion purposes and compliance with applicable law, or to exercise rights thereunder.

If you are offered and accept employment with Branch, the information collected during the application and recruitment process will become part of your employment record.

If You Are a European Economic Area (“EEA”), United Kingdom (“UK”), or Brazil Data Subject, Our Legal Basis for Processing Your Information

We collect and process information you provide us to assess the potential for entering an employment contract with you. Our legal bases for processing your information include: (1) where you have provided consent; (2) where necessary for the performance of a contract with you; (3) for compliance with a legal obligation; or (4) for our legitimate interests in managing and administering business and human resources functions and activities, as described above. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

How Information is Shared

We do not share your personal information except in the limited circumstances described below:

When You Agree or Direct Us to Share

You may agree or direct us to share your personal information with others as part of your employment with Branch. For example, in certain jurisdictions, consent may be legally required for Branch to perform a background check.

For External Processing

We may share your personal data with our employees, contractors, consultants and other parties (including Branch affiliates) who require such information to assist us with establishing, managing or terminating our employment relationship with you. We may also share your personal data with service providers, including technology and analytics providers that assist us with operating our

business, or with other parties in a manner consistent with the use and disclosure provisions of this Policy.

We may also provide your information to another entity (such as a potential or existing business counterparty or customer) with a means of contacting you in the normal course of business, for example, by providing your contact details, such as your phone number and email address.

For Legal Reasons or to Prevent Harm

We may preserve or disclose information about you to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of the Services or the physical safety of any person.

Please note: Our policy is to notify you of legal process seeking access to your information, such as search warrants, court orders, or subpoenas, unless we are prohibited by law from doing so.

Exceptions to our notice policy include exigent or counterproductive circumstances, for example, when there is an emergency involving a danger of death or serious physical injury to a person.

Transfer of Business Assets

If we are involved in an actual or contemplated merger, acquisition, or sale of assets, we may share your information. We will continue to take measures to protect the confidentiality of personal information and give affected users notice before transferring any personal information to a new entity.

Additionally, Branch may share or sell aggregated, de-identified data that does not identify you with our partners and the public. When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you.

How to Access or Delete Your Personal Information

You may contact your local HR representative for information about how to access or delete information Branch stores related to your employment. You may also request information by sending an email to privacy@branch.io, or by leaving a message at +1-650-209-6461.

Retention of Personal Information

For EEA, UK, Brazil, and Korea-based roles, job applications will be deleted within two years unless otherwise required by applicable law.

All other personal information will be retained for as long as necessary to satisfy the purposes for which it was collected. These purposes may include to comply with reporting, legal, and accounting obligations. We determine retention periods by evaluating our legal obligations and our legitimate business interests (such as backing up systems or maintaining our organizational history).

Your Rights Regarding Personal Data

Residents of the European Economic Area, United Kingdom, or Brazil

Applicants and employees within the EEA, UK, and Brazil have certain rights under the GDPR and other applicable data protection laws. These include the right to request access or to update your information, request that it be deleted, or object to Branch using it for certain purposes.

If you wish to exercise a right of access please contact privacy@branch.io. We will respond to any requests in accordance with applicable law, and so there may be circumstances where we are not able to comply with your request.

If you are located within the EEA, UK, or Brazil and you can't find the answer to your question in this policy, you may contact us at privacy@branch.io. Depending on your country of residence, you may also raise any questions or concerns you have regarding your personal information with your local data protection authority.

California Residents

You may also have certain rights regarding your personal information. Subject to certain exceptions, you may request:

- access to your personal information including the right to obtain confirmation that we are processing your personal information and 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 the personal information that we have or will hold about you that is inaccurate;
- deletion or removal of your personal information.

Exceptions to Your Rights: There are certain exceptions to these 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.

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

We also 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 also allows you to limit the use or disclosure of your "sensitive personal information" (as defined in the California Consumer Privacy Act) if your sensitive personal information is used for certain purposes. Please note that we do not use or disclose sensitive personal information other than for purposes for which you cannot opt out under the California Consumer Privacy Act.

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. 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.

Adherence to Branch Policies

Anyone who is hired by Branch will be required to adhere to all Branch policies, where consistent with applicable local law. Failure to adhere to such policies may result in discipline up to, and including, termination. All individuals whose responsibilities include the processing of personal data on Branch's behalf are expected to protect that data by adherence to Branch's Privacy Policy.

If you have any concerns regarding how your data is processed, you can contact Branch's Data Protection Officer at: privacy@branch.io.