



NOTICE TO CALIFORNIA APPLICANTS/EMPLOYEES

Poppy Bank is committed to protecting your privacy. The information that you provide to Poppy Bank (sometimes referred to as “we”, “us” or “our”) is utilized in order for us to (among other things) consider you as an employee, retain you as an employee, and to maintain employment records.

This Notice (“Notice”) applies to our offline and online data collection practices, including when you submit personal information, either directly through us or through third-party websites and recruiters, for purposes of applying for and/or becoming a valued employee at Poppy Bank and in the course of your employment. This Notice is provided pursuant to the California Consumer Privacy Act and its amendments, including the California Privacy Rights Act (collectively, “CCPA”) and explains how Poppy Bank collects, uses, and discloses Personal Information (PI) of California residents that are employees or are applying to a job position at Poppy Bank. If you are not a job applicant or employee who is a California resident, this Notice does not apply to you.

For more information on Poppy Bank’s policies please refer to Poppy Bank’s employee handbook.

Your Consent

Please review this Notice periodically. You should read this entire Notice before submitting information, including personal information, to us in any form. Whenever you submit personal information to us, you consent to the collection, use, disclosure, transfer, and storage of that information in accordance with this Notice.

Collection and Disclosure of Personal Information

All personal information may be used for the purposes stated in this Notice. We may make full use of all information that is de-identified, aggregated, or otherwise not in personally identifiable form.

WHAT WE COLLECT

In the preceding 12 months, Poppy Bank has collected the following categories of Personal Information:

From Job Applicants:

- Name
- Address
- Date of birth
- Telephone number
- Email address
- Signature
- Professional or employment-related information, such as work history and prior employer
- Non-public education information shared by the applicant or employee
- Information about your education and employment history



- Internet or network activity information, if you apply online
- Any other information you may provide or submit to us in the course of the application process

From Employees:

- All of the above from Job Applicants
- Corporate unique identifiers (e.g., employee ID)
- Commercial information, such as transaction information and purchase history (e.g., in connection with travel or other reimbursements [or purchases from Poppy Bank])
- Internet or network activity information, such as browsing history and interactions with our online systems and websites and any Personal Information that you provide while accessing Poppy Bank's technology systems, including on our computers and mobile devices which you use for business purposes. If you choose to use a personal device, Poppy Bank utilizes Microsoft InTune. Microsoft InTune will help provide you with privacy of your personal data, while keeping corporate data and resources protected and secure, and to monitor business activity. For more information on how Microsoft InTune is used, visit Microsoft InTune's page [here](#) to learn more.
- Audio, electronic, visual, and similar information

In the preceding 12 months Poppy Bank has also collected the following categories of Sensitive Personal Information:

From Employees:

- Social Security Number
- Passport number
- Federal identification authorizing work in the United States
- Insurance Policy Number
- Geolocation data, such as device location from usage of the Poppy Bank devices
- Corporate access/password information
- Bank account number and other financial information
- Information regarding your healthcare insurance including medical information
- Characteristics of protected classifications under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language, immigration status, military/veteran status, disability, request for leave, and medical conditions
- Internet or network activity information, such as browsing history and interactions with our online systems and websites and any Sensitive Personal Information that you provide while accessing Poppy Bank's technology systems including, if applicable, personal credit card information and passwords.
- Medical Information and Medical History

Poppy Bank collects Personal Information and Sensitive Personal information from a variety of sources including directly from you; from prior employers, references or recruiters; third-party sources of demographic information; and third-party companies, such as background check companies and drug testing facilities.



PURPOSES FOR COLLECTION

Poppy Bank collects Personal Information and Sensitive Personal Information for a range of purposes including the following:

- To operate, manage, and maintain our business
- To facilitate our payments, to issue paychecks, and to issue reimbursements. Please note that if you choose to also open an account with Poppy Bank as a customer, that account and information will subject to our Consumer Privacy Policy, please click [Here](#) for more info.
- To conduct background checks and conduct drug testing
- For hiring, retention, and employment purposes
- To otherwise accomplish our business purposes and objectives, including, for example:
 - Emergency services
 - Maintaining our facilities and infrastructure
 - Quality and safety assurance measures
 - Conducting risk and security controls and monitoring
 - Protecting confidential and trade secret information
 - Detecting and preventing fraud
 - Performing identity verification
 - Performing accounting, audit, and other internal functions, such as internal investigations
 - Complying with the law, legal process, and internal policies
 - Maintaining records
 - Claims processing
 - Responding to legal requests for information and subpoenas
 - Exercising and defending legal claims
- To confirm your identity for timekeeping purposes
- For security surveillance if you go onto our physical premises
- Any other purposes authorized by the California Privacy Protection Agency, the state of California, or Federal law.

HOW WE DISCLOSE YOUR EMPLOYEE PERSONAL INFORMATION

Service Providers and Contractors

We disclose Personal Information you provide to consultants, service providers, and contractors that we use to support our business and operations who have agreed to keep the information confidential and use it only to provide the applicable service(s) such as vendors that help us communicate with you, vendors that host our website and data, security and fraud detection vendors.

Legal Obligations

We may disclose Personal Information to outside parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests; to identify, contact or bring legal action against someone who may be causing injury to or interfering with our (or others') rights or property; to support any actual or threatened claim, defense or declaration in a case or before any jurisdictional and/or administrative authority, arbitration or mediation panel; or in connection with disciplinary actions/investigations.



Sale or Corporate Restructuring

We may disclose Personal Information to third-parties in connection with the sale, assignment or other transfer of the business of our website or the sale, assignment, merger, reorganization or other transfer of our brand or company.

INFORMATION SOLD OR SHARED

Poppy Bank has not sold or shared Personal Information or Sensitive Personal Information collected in the preceding 12 months to any third party.

Retention of Personal Information

Poppy Bank takes into account the following criteria when defining the duration for which your Personal Information and Sensitive Personal Information will be retained:

- We will retain your Personal Information and Sensitive Personal Information for as long as you are an employee of Poppy Bank or for as long as you participate in the recruiting process of Poppy Bank as an applicant. After termination, former employee Personal Information and Sensitive Personal Information will be stored during a predefined period for the reasons explained below.
- We will retain your Personal Information and Sensitive Personal Information for as long as it is required by any applicable law or regulation.
- Additionally, we might retain your Personal Information and Sensitive Personal Information in connection to any relevant legal claim for the periods necessary to sustain those claims and in relation to any potential regulatory audits or investigations or any other relevant legal matter.

Your Rights as a California Resident

As a California resident, you have the rights described below, with respect to the Personal Information and Sensitive Personal Information we have collected or disclosed about you as an employee or as an applicant to a job position at Poppy Bank.

- **Right to Know and Right to Request Information**

You have the right to request that we disclose what personal information we collect, use, disclose, or sell or share. You have the right to request information about the personal information we've collected about you within the last twelve months. You may request to know if we have collected, disclosed, sold or shared with third parties for a business purpose the following information:

- The categories of personal information we have collected about you.
- The categories of sources of personal information we collected about you.
- Our business or commercial purpose for collecting or selling personal information about you.
- The categories of third parties with whom we share personal information.
- The specific pieces of personal information we have collected about.



- Whether we have sold your personal information and if so the categories of personal information that each category of recipient purchased.
- Whether we have disclosed your personal information for a business purpose and if so, the categories of personal information that each category of recipient received.

You may request this information no more than two times per year.

- Right to Request Correction

You have the right to request that we correct inaccurate Personal Information that we maintain about you.

- Right to Know Sensitive Personal Information Collected

We collect and use your sensitive personal information as described above. We do not collect or process sensitive personal information for the purpose of inferring characteristics. We also do not collect sensitive personal information for any purposes other than those set forth in Regulations promulgated by the California Privacy Protection Agency, Title 11, Div. 6, Chpt. 1, Art. 3, Section 7027(m).

- Right to Request Deletion

You have the right to request that we delete your personal information. Under certain circumstances we may be unable to delete your personal information, for example, to comply with legal obligations, or to fulfill our obligations as an employer.

- Right to Non-Discrimination for Exercising Consumer Privacy Rights

You have the right not to receive discriminatory treatment for exercising your privacy rights conferred by the California Consumer Privacy Act, including by exercising the rights specified herein.

HOW TO MAKE A RIGHTS REQUEST

You have the right make requests for the aforementioned rights (Request to Know; Request to Delete; or a Request to Correct (a “Request”).

To make a Request for any of the information set forth above, please submit a verifiable request pursuant to the instructions below. The Request must provide sufficient information to allow us to verify that you are the person about whom the personal information was collected, sold, shared, or disclosed and must contain sufficient detail to allow us to properly understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request. We will acknowledge your Request within 10 business days and will attempt to respond substantively within 45-90 days.



You may make a Request the following ways:

- You may make a request here: privacy@poppy.bank
- Enter your request here [Trust Arc](#).
- You may also make a request by phone by contacting us at 888.636.9994.

Once we receive your Request, we will begin the process to verify that you are the person that is the subject of the request (the “Verification Process”). The Verification Process consists of matching identifying information provided by you with the information we have about you in our records. You will be asked to provide us with two or three pieces of information that will help us to verify your identification.

We will review all information provided by you to us, to determine whether we can respond to your Request. We will inform you of our decision to deny or grant your Request.

For any Requests to Know, you may make such Requests twice within a 12-month period.

For Requests to Correct, you will need to provide evidence supporting the inaccuracy of the current information, and we reserve the right to delete the information instead of correcting if such deletion does not impact you or you consent to the deletion.

We will retain correspondence, documents and information related to any Request for 24 months as required by law.

AUTHORIZED AGENT INFORMATION

You may designate an authorized agent to make a request on your behalf under the California Consumer Privacy Act.

In order to allow an authorized agent to make a request on your behalf, please email Human Resources at privacy@poppy.bank or call 888-636-9994 and provide your written request and consent to an authorized agent.

When your authorized agent makes a request related to your personal information, we will require the agent to provide the above written permission. We may also require that you verify your own identity directly with us at the time such a request is made.

GOVERNING LAW

This Notice along with our privacy practices will be subject exclusively to the laws of the State of California, United States of America. We make no representation that this Notice and its practices comply with the laws of other jurisdictions.

Changes to this CCPA Privacy Policy

Changes to this policy may be made at any time. When changes are made, the revised Policy will be communicated to all employees and will include a new “Effective” date.



Contact Us

If you have questions regarding your rights under the CCPA, please email us at privacy@poppy.bank or writing to us at:

Poppy Bank
438 First Street
Attention: Compliance Department
Santa Rosa, CA 95401