BREMER BANK

Bremer California Employee Notice at Collection and Privacy Policy

Bremer Bank, National Association and Bremer Insurance Agencies, Inc. (“Bremer”) collects, maintains, and uses Personal Information about job applicants, employees, independent contractors, owners, directors, and officers of Bremer who are California residents (“Employees”). Bremer provides this California Employee Notice at Collection and Privacy Policy (“Notice and Policy”) to inform you about the categories of Personal Information to be collected and the purposes for which the categories of Personal Information will be used as a Bremer Employee.

In this Notice and Policy, any use of the words "you," "yours," or similar expressions refers to our Employees. References to "we," "us,” "our" or similar expressions refer to Bremer. The term “Personal Information” means information that identifies, relates to, or could reasonably be linked with a particular California resident or household as defined under the California Consumer Privacy Act; CA CIVIL § 1798.100, et seq., as amended from time to time and its implementing regulations (the “CCPA”).

Summary of Bremer’s Privacy Practices

1. Information sources for Employees
Bremer collects Personal Information about Employees from the following sources: Employees, service providers, contractors, affiliates, government entities and operating systems and platforms. We may also collect Personal Information about an employee’s spouse, dependents, beneficiaries, emergency contacts, and other individuals relevant to Employee.

2. Information we collect about Employees
2.1 INFORMATION WE COLLECT AND RECEIVE
Bremer may have collected the following categories of Personal Information about Employees in the last 12 months.

- Identifiers such as name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, signature, telephone number, or other similar identifiers.
- Characteristics of protected classifications, such as family information (e.g., marital status, relevant information on spouse/dependents); benefits information (e.g., wellness information, COBRA information, healthcare plan information, insurance information); disability claims records (e.g., workers’ compensation records and disability claims records); medical reports or records (e.g., pre-employment drug tests, medical benefits-related documentation); or certain physical characteristics (e.g., age, disability, race, color, gender).
- Professional information, such as employment history, employment verification information, promotions, service dates, training information, length of service, compensation, tax information, bank account data, current department/position, employment status, job performance, attendance records, disciplinary actions, recordings of customer servicing calls, relocation information, employee development information, payroll information, or other employment-related information.
- Education information, such as resume and application information, education verification information, level of education, degrees received, certifications, etc.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, online applications used, and information regarding an Employee's interaction with an Internet website, application, or advertisement.
- Geolocation information, such as the location of you or your device.
- Inferences drawn from any of your Personal Information to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes, such as inferences about your job performance, disciplinary determinations, or professional development.
- Audio or visual information such as the content of video interviews and conferences, security cameras, call recordings, etc.

- Sensitive Personal Information, including but not limited to, date of birth, sex, racial and ethnic origin, Veteran status, Social Security number, driver's license, state identification card, passport number, health and medical records, disability information, benefits information, insurance coverage, login credentials, contents of Employee mail and email, and financial account information.
- Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies.

2.2 COOKIES AND TRACKERS

We use cookies and other tracking technologies (e.g., web beacons, pixels, ad tags and device identifiers) to recognize you and/or your device(s) on, off, and across our website at bremer.com (the "Site") and different devices. You may be able to control certain cookies through your browser settings and other tools. Our Site does not respond to Do Not Track signals.

Third parties may also use cookies and other tracking technologies to assist us with our Site and services. For example, Google may place cookies for analytics and marketing purposes. You can opt-out of Google tracking through Google Ads Settings, Ad Settings for mobile apps, or any other mechanisms Googles makes available, such as the Google Analytics opt-out plug-in for the web. For more information about how you may be able to opt-out of certain online behavioral advertising, please visit aboutads.info/choices/, networkadvertising.org/, or youronlinechoices.com.

3. How we use information about Employees

We use the Personal Information about Employees for the following business purposes:

- Performing human resource functions, including processing job applications, administering benefits, processing payroll, conducting analytics, or managing other aspects of an employment relationship including, but not limited to, the establishment, maintenance, and termination of employment relationships.
- Determining eligibility for initial employment, including the verification of references and qualifications.
- Processing background checks of new applicants and existing Employees.
- Managing the terms and conditions of employment, such as payment of wages/salary, direct deposit authorization, the provision and administration of benefits and leaves of absence, and maintenance of emergency and beneficiary contact information.
- Processing Employee work-related claims (e.g., worker compensation, insurance claims, etc.).
- Conducting training, taking disciplinary action, addressing injuries, and other employment related incidents.
- Providing a safe work environment.
- Administering our occupational safety and health programs.
- Assisting you with obtaining immigration or work documentation, when required.
- Maintaining directories of Employees.
- For employee-related programs, including surveys and voluntary programs.
- Investigating and responding to claims against us.
- For corporation transactions, such as transferring Personal Information in the event we sell or transfer, or are considering selling or transferring, all or a portion of our business or assets.
- Auditing compliance.
- Helping to ensure security and integrity to the extent the use of your Personal Information is reasonably necessary and proportionate for these purposes.
- Debugging to identify and repair errors that impair existing intended functionality.
- Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of your current interaction with Bremer.
- Performing services on behalf of Bremer, including maintaining or servicing accounts, providing services, verifying information, processing payments, providing storage, or providing similar services on behalf of Bremer.
- Providing advertising and marketing services, except for cross-context behavioral advertising, to you.
- Undertaking internal research for technological development and demonstration.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the Bremer, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the Bremer.
- Complying with federal, state, or local laws or comply with a court order or subpoena to provide information.
- Complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

- Cooperating with law enforcement agencies concerning conduct or activity that Bremer, its service providers, or third parties reasonably and in good faith believe may violate federal, state, or local law.
- Cooperating with a government agency request for emergency access to an Employee's Personal Information.
- Exercising or defending legal claims.
- For any other purpose not otherwise prohibited by applicable law.

4. How information may be disclosed about Employees
For any of the above business purposes, we may disclose any of the categories of Personal Information that we collect about Employees to service providers, contractors, affiliates, government entities, operating systems and platforms. We do not sell, share or rent any of your Personal Information and we do not disclose your Personal Information publicly without your consent.

5. Protection of Your Information
We follow industry-standard practices to protect the data we collect and process. Bremer has therefore put in place commercially reasonable physical, electronic, and managerial procedures to safeguard and secure the Personal Information that Bremer collects. Access to Personal Information will be restricted to our authorized personnel who require the information in order to perform their duties properly. In addition, access will be limited to only that information that is strictly necessary for the performance of those duties.

Remember, the safety and security of your information also depends on you. Where you have chosen, or where we have given you a username and password for access to certain parts of the Site or services, you are responsible for keeping the username and password confidential. No method of transmission over the internet or electronic storage is completely secure, so Bremer cannot guarantee its absolute security.

6. Employee Rights
Except where an exemption applies, you have certain rights as an Employee that include 1) the ability to request a copy of the information we have collected about you during the previous 12 months, as well as the right to review our data collection practices related to you, (a "Personal Information Request"); 2) the ability to request deletion of your Personal Information that we have collected from you; 3) the ability to correct your inaccurate Personal Information maintained by us; 4) the ability to opt out of our selling or sharing of your Personal Information; 5) the ability to limit the use and disclosure of Sensitive Personal Information; and 6) the right not to be discriminated or retaliated against due to your exercise of any of the preceding rights. While these rights are not globally applicable, our Employees are entitled to submit requests.

How to submit requests
You may call us at 800-908-2265 or 651-288-3751 or email us at peopleresourcenter@bremer.com to exercise any of these rights. To protect your privacy and security, Bremer may take reasonable steps to verify your identity before granting access to, correcting, or deleting data. As part of our verification procedures, we may request that you provide the following information to identify yourself: name, contact information, Social Security or individual taxpayer identification number, date of birth, cell phone number, email, user ID, business ID, password, account number. We will attempt to match information that you provide in making your request with other sources of similar information to reasonably verify identity. In addition, for certain requests, we may require an extra layer of verification such as requiring you to sign a declaration under penalty of perjury that you are the Employee whose Personal Information is the subject of the request.

Requests by authorized agents
An Employee may designate an authorized agent to make a request on behalf of the Employee by contacting us at the toll-free number or email address listed above. If you designate an authorized agent to make an access, correction, or deletion request on your behalf, we may require you to provide the authorized agent written permission to do so and require you to verify your own identity directly with us (as described above).

As part of our verification process, we may request that the authorized agent provide:
- The authorized agent's name; contact information; Social Security or individual taxpayer identification number; date of birth; and government issued ID, such as driver's license, State ID, passport, or Matricula Card.
- The name; contact information; Social Security or individual taxpayer identification number; date of birth; and the government issued ID of the Employee on whose behalf the request is being made.
- A document to confirm that the authorized agent is authorized to make the request such as a copy of a power of attorney, legal guardianship or conservatorship order, or a birth certificate of a minor if the requestor is the custodial parent.

- For an authorized agent of a company or organization ("legal entity agent") making a request on behalf of an Employee:
    - The legal entity agents' active registration with the California Secretary of State.
    - Proof that the Employee has authorized the legal entity agent to make the request.
    - The name; contact information; Social Security or individual taxpayer identification number; data of birth; and government issued ID of the Employee on whose behalf the request is being made.
    - From the individual who is acting on behalf of the legal entity requestor, proof that the individual is authorized by the legal entity requestor to make the request.

Our response to requests
We will generally respond to your request within 45 days, unless, for reasons beyond our control, a longer response time is necessary, in which case, you will be advised accordingly. Please note that we may retain certain information about such requests as required by law or as necessary for our legitimate business purposes.

7. Questions, comments, or complaints
If you have questions or comments about this Notice and Policy, or if you are not completely satisfied with this Notice and Policy or its application by us, or any of our determinations in response to your request(s), we invite you to convey your concerns or suggestions to us at 800-908-2265 or 651-288-3751 or email us at peopleresourcenter@bremer.com. We will reply as quickly as possible and inform you of the steps, if any, that have been or will be taken in order to address your concern or implement the suggestion.

If you have a disability that prevents or limits your ability to access these privacy disclosures, please contact us so we can work with you to provide these disclosures in an alternative format.

8. Updates and Changes to this Notice and Policy
The privacy practices described in this Notice and Policy are effective as soon as posted or provided to you as indicated by the Last Updated date below. Should we change any of the practices described in this Notice and Policy, we will notify you by posting the changes to the Site or as otherwise required by applicable law. Your continued employment with us following any such changes will constitute your agreement to these privacy practices.

This Notice and Policy goes into effect on January 1, 2023. We may change this Notice and Policy from time to time, and the most current version will be available on our Site. You understand that by continuing to be our Employee after the effective date of any change, you have agreed to the most recent version of this Notice and Policy.

Last updated: February 2, 2023