

Employee and Applicant Privacy Notice

Effective Date/Last Updated: May 25, 2023

This Employee and Applicant Privacy Notice describes the types of information that Restaurant Services Group, Inc., FQSR, LLC d/b/a KBP Foods, KBP Bells, LLC, KBP Inspired, LLC, and our affiliates and subsidiaries, along with the nonprofit entity KBP Cares, Inc. (collectively, “KBP”, “we”, “us”, or “our”), collect from job applicants and employees, how we use that information, and how we may share that information.

This Notice does not constitute an offer or contract for employment. Parts of this Notice dealing with employees do not apply to applicants unless they become employees.

1. Personal Information We Collect

We may collect a range of Personal Information. “Personal Information” means information that uniquely identifies, relates to, describes, or is reasonably capable of being associated with or linked to you. We collect the following types of Personal Information when you apply for a job and/or during employment:

- Your name, address, email address, telephone number, and other contact information;
- Your resume or CV, cover letter, previous and/or relevant prior experience, education, transcripts, or other information you provide us during the application and recruitment process;
- Information from interviews;
- Details of the type of employment you are looking for, current and/or desired salary and other terms relating to compensation and benefits packages, and job preferences;
- Details of how you heard about the position you are applying for;
- Sensitive and/or demographic information, such as gender, citizenship and/or nationality information, medical or health information, and/or your racial or ethnic origin;
- Personal identification numbers, such as your Social Security number, driver’s license number, password, pass codes or employment ID number;
- Reference information and/or information received from background checks (as applicable), including information provided by third parties;
- Information from prior applications or employment with any KBP company;
- Information about your educational and professional background from publicly available sources (e.g., your LinkedIn profile);
- Banking information for direct deposit purposes, income history and income information, and benefits information, including about your beneficiaries; and
- Information collected from you automatically when you use our website, while using a KBP device, or while connected to KBP’s Internet or job application site through cookies, web beacons, pixel tags, and other online tracking mechanisms.

2. Information Collected from Other Sources

We obtain information from various third-party and public sources and may combine that data with Personal Information. For example, KBP may collect:

- Application information from recruiters;
- Information about your past employment from former employers;

- Information about your citizenship or eligibility to work in the country where you would be employed from government agencies;
- Credit history and/or criminal record if you consent to a background check;
- Information about your qualifications to work with KBP from your references;
- Information from third party websites (such as, Indeed and LinkedIn, etc.);
- Drug test results from the third-parties who perform drug tests; and
- Health information, including your fitness to carry out work and/or any accommodations or adjustments to be considered from your medical provider.

3. Children Under 16

We only employ those who are legally eligible to work where employed. Please do not send us application materials if you are under the age of eligibility to be employed in the state in which you reside.

4. Purposes for Which We Collect Personal Information

KBP processes your Personal Information for the following purposes:

- **To Manage the Application Process.** We use your Personal Information to process and verify the information in your job application and to confirm your eligibility for a position. We may also save your information for future job openings within KBP.
- **To Manage the Hiring Process.** We may use your Personal Information to conduct interviews, check your references or obtain background checks (with your authorization and in accordance with applicable law). We may also use it to communicate with you about the recruiting process, to learn where you heard about KBP, or to evaluate and improve our recruiting process.
- **To Communicate with You.** We may use your Personal Information to provide you with information, answer your questions, to notify you of changes to your compensation and benefits program or to notify you of emergencies.
- **To Manage the Onboarding Process.** For new hires, we will collect Personal Information when you complete new hire paperwork to assist us in administering salary and benefits and to assist us with complying with government and/or legal requirements.
- **To Administer Compensation and Benefits Programs.** We will use the Personal Information you provide to process payroll, pay taxes, help employees address employment related tax issues, administer benefits and handle work related expense reimbursement. We also use Personal Information to administer employee claims under programs like workers' compensation or unemployment benefits. We may also use Personal Information to provide work-related accommodations.
- **For Performance Management.** KBP collects Personal Information to assess (and improve) your performance, assist in career development, conduct pay and grading reviews, and to handle employment related disputes. We may also use Personal Information to respond to complaints, investigate potential violations of company policies and to gather information for disciplinary actions. We may monitor any activity you perform online while using a KBP device or while connected to KBP's Internet, including the websites you visit and your activity on those websites when using a KBP device or internet connection. We may also track the emails you send using

your KBP-provided email address, the phone calls you make using a KBP-provided device, and the chat messages you are involved in when using the KBP-provided instant messaging program.

- **Law Enforcement and Courts.** We may disclose your Personal Information in response to a subpoena, a search warrant or other legally valid process. We may use your Personal Information to cooperate with law enforcement or other government entities if you are suspected of having violated the law.
- **Record Keeping.** We may use Personal Information to comply with record keeping requirements and to respond to requests for information from government entities.
- **Health and Safety.** We may use Personal Information to protect your health and safety, or the health and safety of others, including through the use of technology to allow contact tracing if you may have been exposed to communicable diseases such as COVID-19. We may also use this information to respond to an employee related emergency. We may also use this Personal Information to protect our facilities and personal property.
- **Protect Our Legal Rights.** We may use your Personal Information to protect our legal rights, to defend a claim or lawsuit, and to investigate or prevent actual or suspected loss or harm to persons or property. We may use your Personal Information to seek legal, accounting or other professional advice or to identify, contact or bring a legal action against someone who may cause or is causing harm to or interfering with the legal rights of KBP or any other party.
- **Security.** We may use your Personal Information to monitor the use of our information systems and electronic resources, to conduct internal audits or investigations and for safety and security of KBP employees, visitors and facilities. We also may use such information to protect KBP against illegal activity and misconduct such as fraud, deceptive practices and data security incidents. We use this to offer, operate, maintain, deliver, troubleshoot and update our websites, programs, network and systems used by KBP in the course of its business.

5. How We Share Your Personal Information

We share your Personal Information in the following circumstances:

- **Within KBP.** We may share your Personal Information internally within KBP and among KBP's affiliates for recruiting and/or evaluating applicants, resource planning, and for talent and recruiting, human resources and business administration functions. All KBP employees who access or process Personal Information must comply with KBP's privacy and security policies.
- **Service Providers.** KBP may share Personal Information with third-party service providers or suppliers ("Service Providers") such as background screening providers, employee benefits providers, data storage providers, website or mobile application hosting providers, and e-mail service providers. KBP will take steps to help ensure appropriate protections are in place before we share or disclose Personal Information with any Service Provider.
- **Legal Requirements.** We will cooperate with law enforcement and other governmental agencies. We may disclose Personal Information as necessary to meet our legal obligations, including the following:
 - If we believe in good faith we are legally required to disclose that Personal Information;

- If we are advised to disclose Personal Information by our legal counsel;
 - When necessary to identify, contact or bring a legal action against someone who may cause or be causing harm to, or interfering with the legal rights of, KBP or any other party;
 - For tax and payment purpose (e.g. Internal Revenue Service);
 - To protect our rights or property, your health and safety, or the health and safety of others;
 - To detect and investigate fraud or illegal activity, or to respond to a government request; or
 - To respond to an emergency.
- **Professional Advisors.** We may share Personal Information with our professional advisors, such as our attorneys and accountants, in their capacity as advisors, including for advice on potential or actual litigation matters.
 - **Change in Ownership.** We may use and disclose Personal Information in connection with the evaluation of a change of control of KBP, such as in the event of a merger, acquisition, or sale of assets. We may provide Personal Information both in connection with a due diligence process or it could be transferred as part of the change of control to subsequent owner(s). If we (or our assets) are acquired or if we go out of business, enter bankruptcy, or go through some other change of control or reorganization, Personal Information and other information could be one of the assets transferred to or acquired by a third party, or reviewed as part of the due diligence process.

6. De-Identified/Aggregate Information

We may collect or create information that is de-identified or aggregate information that does not identify a natural person (“De-Identified Information”). KBP is the sole and exclusive owner of De-Identified Information and may use or share such information for any legal business purpose. For example, KBP may create aggregated information about applicants to learn about the success of its recruiting processes.

7. Data Security

We protect Personal Information using technical and organizational measures designed to reduce the risks of loss, misuse, and unauthorized access, disclosure, alteration, and destruction of Personal Information appropriate to the type of Personal Information processed.

Still, it is impossible to guarantee 100% security in all circumstances. KBP employees and applicants are responsible for safeguarding the security of any password, user ID, or other form of authentication they use to obtain access to password-protected or secure areas of any KBP-owned or licensed platforms.

If you have reason to believe that your interaction with us is no longer secure, you must immediately notify us. If a breach of your Personal Information occurs, we will notify you of the breach if and as required under applicable law. To protect you and your Personal Information, KBP may suspend your use of any KBP programs or platforms without notice if any breach of security is suspected.

8. Retention of your Personal Information

Personal Information will be stored as required by law and to carry out the purposes described in this Notice. Generally, for employees, this means your Personal Information will be retained until the end of your employment or work relationship plus a reasonable period of time thereafter to respond to work-related inquiries or to deal with any legal matters, document the proper termination of your work relationship, or

to provide you with any ongoing benefits. For more specifics on how long information is retained, please see our Human Resources Records Retention Policy.

We retain biometric information of employees in accordance with our Biometric Policy, Notice and Consent.

For job applicants, unless you become an employee, we will retain your Personal Information for two years from the date you provide such Personal Information.

Personal Information that will no longer be kept will be securely and effectively destroyed, such as through shredding or permanently erasing the information from our systems. We will also inform third parties of their obligations to destroy or erase such Personal Information where applicable.

9. A Note on Social Security Numbers

Access to applicant or employee social security numbers is limited to only those with a valid business or legal purpose to ensure they are kept confidential. Any unlawful disclosure of social security numbers is prohibited. Anyone who unlawfully discloses an applicant or employee social security number will be subject to discipline, up to and including termination.

10. California Employees/Applicants

This Section applies to our collection and use of Personal Information if you are a resident of California, as required by the California Consumer Privacy Act of 2018 and its implementing regulations, as amended by the California Privacy Rights Act (the “CPRA”). This Section describes (1) the categories of Personal Information, collected and disclosed by us, subject to CPRA, (2) your privacy rights under CPRA, and (3) how to exercise your rights.

If you would like to receive a copy of this Section in an alternate format (e.g., printable) or language, please contact us using the information provided in the Contact Us section below.

KBP makes the following disclosures about the Personal Information KBP has collected within the 12-month period preceding the Effective Date of this Notice:

Sources of Personal Information

We collect Personal Information directly from you and from the sources detailed in Section 2 above.

Use of Personal Information

We collect Personal Information for the business purposes detailed in Section 4 above.

Disclosure of Personal Information

The categories of third parties to which we disclose Personal Information for a business or commercial purpose or to whom we sell or share Personal Information are summarized in the chart below. We do not knowingly sell or share the personal information of applicants, employees, or minors under the age of 16.

For applicants who are not hired, this information is kept for two years from date provided. For employees, please see the Human Resources Records Retention Policy. We do not sell or share Personal Information.

Categories	Examples	Disclosed To
Identifiers	Real name, alias, mailing address, unique personal identifier, online identifier, Internet Protocol address (“IP address”), email address, account name, Social Security number, driver’s license number, passport number, or other similar identifiers.	Affiliates, service providers; public or governmental authorities; etc.
Personal information, as defined in the California customer records law	Name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Affiliates, service providers; public or governmental authorities; etc.
Commercial Information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Affiliates, service providers; public or governmental authorities; etc.
Biometric Information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	Affiliates, service providers; public or governmental authorities; etc..

Characteristics of protected classifications under California or Federal Law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	Affiliates, service providers; public or governmental authorities; etc.
Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	Affiliates, service providers; public or governmental authorities; etc.
Geolocation data	Physical location or movements.	Affiliates, service providers; public or governmental authorities; etc.
Audio, electronic, visual, thermal, olfactory, or similar information		Affiliates, service providers; public or governmental authorities; etc.
Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Affiliates, service providers; public or governmental authorities; etc.
Professional or employment-related information	Current or past job history or performance evaluations.	Affiliates, service providers; public or governmental authorities; etc.

<p>Non-public education information (per the Family Education Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99))</p>	<p>Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.</p>	<p>Affiliates, service providers; public or governmental authorities; etc.</p>
<p>Sensitive personal information</p>	<p>Social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; genetic data; biometric information for the purpose of uniquely identifying a consumer; personal information collected and analyzed concerning a consumer's health; or personal information collected and analyzed concerning a consumer's sex life or sexual orientation.</p>	<p>Affiliates, service providers; public or governmental authorities; etc.</p>

If you are a resident of California, you have the following rights:

Privacy Right	Description
Notice	<p>The right to be notified of what categories of Personal Information will be collected at or before the point of collection and the purposes for which they will be used and shared.</p>
Access	<p>The right to request the categories of Personal Information that we collected in the previous twelve (12) months, the categories of sources from which the Personal Information was collected, the specific pieces of Personal Information we have collected about you, and the business purposes for which such Personal Information is collected and shared. You may also have the right to request the categories of Personal Information which were disclosed for business purposes, and the categories of third parties in the twelve (12) months preceding your request for your Personal Information.</p>

Data Portability	You may have the right to receive a copy of your information in a portable and readily usable format.
Erasure	The right to have your Personal Information deleted. However, please be aware that we may not fulfill your request for deletion if we (or our service provider(s)) are required or permitted to retain your Personal Information for one or more of the following categories of purposes: (1) to complete a transaction for which the Personal Information was collected, provide a good or service requested by you, or complete a contract between us and you; (2) to ensure our website integrity, security, and functionality; (3) to comply with applicable law or a legal obligation, or exercise rights under the law (including free speech rights); or (4) to otherwise use your Personal Information internally, in a lawful manner that is compatible with the context in which you provided it.
Correction	You have the right to request that we correct any incorrect Personal Information that we collect or retain about you, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see below), we will correct (and direct any of our service providers that hold your data on our behalf to correct) your Personal Information from our records, unless an exception applies. We may deny your correction request if (a) we believe the Personal Information we maintain about you is accurate; (b) correcting the information would be impossible or involve disproportionate effort; or (c) the request conflicts with our legal obligations.
Automated Decision Making	You have the right to request information about the logic involved in automated decision-making and a description of the likely outcome of processes, and the right to opt out. KBP does not currently engage in any automated decision-making practices.
To Opt Out of Sales or Sharing of Personal Information	We do not sell or share your Personal Information. However, if we did, you would have the right to opt out of the sale or sharing of your Personal Information.
Limit Use of Sensitive Personal Information	You have the right to limit the use of your sensitive Personal Information (e.g. Social Security number and driver's license information) to only employment related purposes.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a request related to your Personal Information.

You may only make a request for access or data portability twice within a 12-month period. The request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative; and
- Give enough detail to allow us to understand, evaluate, and respond to it.

To submit a request, please email us at hsupport@kbpbrands.com or contact us at (888) 971-2991.

If we cannot initially verify your identity, we may request additional information. We will only use Personal Information provided in a request to verify the requestor's identity. If you are an authorized agent making a request on behalf of a California consumer, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney. Making a verifiable consumer request does not require you to create an account with us.

We endeavor to respond to requests within forty-five (45) days, unless the request is to opt-out of the sale of Personal Information, in which case we will respond within fifteen (15) days. If we need more time, we will inform you of the reason and extension period in writing.

We will deliver our written response via e-mail.

We do not charge a fee to process or respond to your request unless it is excessive, repetitive, or unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

We may deny certain requests, or only fulfill some in part, as permitted or required by law. For example, if you request us to delete Personal Information, we may retain Personal Information that we need to retain for legal purposes.

You will not be discriminated against in any way by virtue of your exercise of the rights listed in this Notice, which means we will not deny goods or services to you, provide different prices or rates for goods or services to you, or provide a different level or quality of goods or services to you.

11. Changes to this Notice

We may change this Notice from time to time, and we will post any changes on this page. Each version of this Notice is identified at the top of the page by its Effective Date.

12. Contact Us

For any questions or concerns, please contact us at hrrsupport@kbpbrands.com. You may also write to us via mailing mail at:

KBP Human Resources
11141 Overbrook Road, Suite 400
Leawood, KS 66211