EMPLOYEE PRIVACY POLICY

Last modified June 27, 2023

1. Purpose.

JBS USA Food Company and its subsidiaries and affiliates (collectively, "**we**", "**us**" or "**our**") respects its employees and understands that you are concerned about privacy and the use of your personal information. We are committed to respecting your privacy, and this Privacy Policy (this "**Policy**") describes how we collect, use, protect and share personal information that we receive as part of your employment with us.

Please read this Privacy Policy carefully. As part of your employment, you consent to our collection, use and sharing of your information in accordance with this Privacy Policy. If you have questions about this Privacy Policy or our use of your information, please send us a message at JBS.Compliance@jbssa.com or, if you are an employee of Pilgrim's Pride Corporation, Pilgrims.Compliance@pilgrims.com.

2. Personal Information We Collect.

As part of your employment at JBS, we may collect certain Personal Information about you. "**Personal Information**" is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, whether directly or indirectly, with a particular person. Below are the categories of Personal Information we may collect about you:

- Identifying information, such as your full name, gender, date of birth, and signature;
- Demographic data, such as race, ethnic origin, marital status, disability, and veteran or military status;
- Contact information, such as your home address, telephone numbers, email addresses, and emergency contact information;
- Dependent's or other individual's information, such as their full name, address, date of birth, Social Security numbers (SSN), and tax information;
- National identifiers, such as SSN, passport and visa information, and immigration status and documentation;
- Educational and professional background, such as your work history, academic and professional qualifications, educational records, references, driving history and records, professional licenses, criminal history and interview notes and messages;
- Employment details, such as your job title, position, hire dates, compensation, performance and disciplinary records, and vacation and sick leave records;
- Financial information, such as banking details, tax information, payroll information, and withholdings;
- Health and safety information, such as health conditions (if relevant to your employment), job restrictions, workplace illness and injury information, and health insurance policy information;
- Information Systems (IS) information, such as your search history, browsing history, login information, and IP addresses on JBS's information systems and networks, of any device connected to our network or systems;
- Internet or other similar network activity, such as browsing history and search history, of any device connected to our network or system;
- Biometric information, such as fingerprints, face patterns, and voice and video recordings;
- Geolocation data, such as physical location or movements;
- Commercial information, such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Sensory data, including audio, electronic, or visual information or temperature checks;
- Surveillance information, such as call monitoring and video surveillance;

- Inferences drawn from other Personal Information, such as profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes; and
- Sensitive Personal Information, such as your SSN, state ID card, racial origin, religious beliefs, and union membership.

3. <u>How We Use Your Personal Information</u>.

Please note, JBS does not sell your Personal Information and will not use your Personal Information to make any automated decisions affecting you. JBS does and will use and process your Personal Information that it collects and receives to:

- Recruit and evaluate job applicants and candidates for employment;
- Conduct background checks;
- Confirm your licensure status, standing and/or admission;
- Assess possible inclusion in any affirmative action programs, including programs for veterans or individuals with disabilities;
- Manage your employment relationship with us, including for:
    - onboarding processes;
    - timekeeping, payroll, and expense report administration;
    - employee benefits administration, such as evaluating and permitting your participation in any retirement plan or benefits offered by JBS in which you or your dependents are eligible to participate and administering your participation in and payments made to or from such plan or benefits;
    - employee training and development requirements;
    - the creation, maintenance, and security of your online employee accounts;
    - notifying your emergency contacts when necessary;
    - workers' compensation claims management;
    - employee job performance, including goals and performance reviews, promotions, discipline, and termination; and
    - other human resources purposes, such as to track the use of vacation, sick days, disability or leave policies, or employee communication;
- Administer and maintain JBS's operations, including health and safety purposes;
- Conduct internal audits and workplace investigations;
- Administer our personnel policies and assess risk management issues;
- Manage and monitor employee access to JBS facilities, equipment, and systems for purposes such as:
    - To help maintain the safety, security, and integrity of JBS's websites, products, services, applications, databases, networks, and other technical assets;
    - To debug, identify, rectify, or mitigate errors or vulnerabilities in JBS's website, systems, applications, technologies, hardware, software, servers or equipment;
    - To protect the operations of JBS, or the safety, security and privacy of JBS and its employees, clients or third parties;
    - To evaluate and resist malicious, deceptive, fraudulent or illegal actions directed at JBS or the information in our possession and to prosecute anyone responsible;
- Investigate and enforce compliance with and potential breaches of JBS policies and procedures;
- Engage in corporate transactions requiring review of employee records, such as for conducting due diligence or evaluating, negotiating, documenting, settling or closing a deal, merger, acquisition, contract or legal dispute
- Maintain commercial insurance policies;
- Communicate with you or a privileged third party such as an attorney, insurance companies, insurance brokers and carriers, insurance agency, benefits or claims administrators, adjusters, concerning the investigation and/or legal analysis of any claim or dispute;

- Perform workforce analytics, data analytics, and benchmarking;
- For client marketing purposes;
- Exercise or defend the legal rights of JBS and its employees, customers, contractors, and agents;
- Review, confirm and evaluate the identity of a person making a request concerning information in JBS's possession;
- Comply with all federal, state or local laws and regulations;
- Comply with any legal obligation imposed upon us by law or by a legal demand or lawful order;
- Defend, prosecute, or respond to a lawsuit, administrative proceeding, or claim; and
- For any purpose related to any of the foregoing.

4. Security.

We are committed to preventing others from unauthorized access to the personal information you provide to us and that we have in our possession. In order to protect and ensure the integrity of your information, we maintain administrative, technical and physical safeguards designed to protect personal information against accidental, unlawful or unauthorized access, destruction, loss, alteration, disclosure or use, including, but not limited to:

(a) Updating and testing our technology on a regular basis in order to improve the protection of customer information;
(b) Requiring outside companies and independent contractors to whom we provide customer information for marketing, servicing or processing purposes to restrict the use of the information to those purposes and we prohibit independent use of such information; and
(c) Restricting access to your information through the implementation of internal procedures and policies about the proper physical security of workplaces and records.

Although we will take reasonable security precautions regarding your personal information, you play a significant role in protecting your information as well, such as protecting the security of your user name and password.

5. Changes to this Policy.

The practices and policies contained in this Policy are subject to change and may be modified by us at any time. In the event of any change, we will post and/or provide the revised notice. We reserve the right to change, amend and update this Policy at any time in our sole and absolute discretion, and such changes will be effective upon the providence and/or posting of the revised notice.

6. Privacy Rights.

Depending on where you live, you may have additional rights under your state's data privacy laws. For further state-specific data privacy rights, please see the attached policy(ies).

7. How to Contact Us.

If you have any questions or concerns regarding this Policy and/or our information and data collection and use practices, you can contact us at JBS.Compliance@jbssa.com or, if you are an employee of Pilgrim's Pride Corporation, Pilgrims.Compliance@pilgrims.com, or at:

JBS USA Food Company
1770 Promontory Cr.
Greeley, Colorado 80634
Attn: Ethics & Compliance Department

STATE SPECIFIC RIGHTS

California Employees.

This California Consumer Privacy Statement (this "**CA Privacy Statement**") supplements the Policy and applies solely to employees who are California residents. This CA Privacy Statement uses certain terms that have the meanings given to them in the California Privacy Rights Acts and its implementing regulations, as each is amended, modified or updated (the "**CPRA**").

If you are a California resident, the CPRA provides you with additional rights regarding our use of your Personal Information, subject to exclusions from the rights granted under California law with respect to certain information governed by certain sector-specific privacy laws.

1. Sources of Personal Information.

During the previous twelve (12) month period, we may have obtained personal information about you from any of the sources identified in the Privacy Policy, including, the following categories of sources: (a) directly from you, such as part of your employment; (b) from your devices, such as when you connect to our network; (c) our affiliates and subsidiaries; (d) vendors who provide services on our behalf; (e) data analytics providers; (f) government entities; (g) operating systems and platforms; (h) social networks; or (i) data brokers.

2. How We Use Your Personal Information.

In addition to the uses stated in Section 3 of the Policy, we may also use the categories of Personal Information listed in Section 2 of the Policy for any of the business purposes identified in the CPRA. We will not collect additional categories of personal Information or use the personal information we collect other than for the purposes stated in the Policy or this CA Privacy Statement or for materially different, unrelated, or incompatible purposes without first providing you notice.

3. Retainment of Information.

The length of time we retain your information depends on the nature of the information and the context in which it was received. We will retain your information for as long as necessary during your employment at our company or as required by law. Additionally, we may keep your information for as long as is necessary to comply with our obligations, to resolve disputes, to protect ourselves in the event of a legal claim, and to enforce our agreements, subject to compliance with all applicable laws.

4. California Employee Privacy Rights.

Subject to certain exceptions under the CPRA, California residents may have the following rights with respect to their personal information collected by us:

- **(a) The right to know and access.** California residents have the right to request we disclose: (i) a copy of the personal information that we collect about you; (ii) the categories of personal information that we collected about you in the preceding twelve (12) months; (iii) the categories of purposes for which such personal information was disclosed in the preceding twelve (12) months; (iv) the categories of sources such personal information was collected for; and (v) the categories of third parties such personal information may have been shared with.
- **(b) The right to deletion.** California residents have the right to request that we delete the personal information that we or our vendors collected about you. There may be circumstances under which we will be unable to delete your personal information, such as if we need to comply with our legal obligations. If we are unable to comply with your request for deletion, we will let you know the reason why.

(c) The right to correct inaccurate information. California residents have the right to request that a business maintaining inaccurate personal information about the resident correct that inaccurate personal information.

(d) The right to opt-out of the sale or sharing of personal information. California residents have the right, at any time, to direct a business that sells or shares his or her personal information not to sell or share such information. Please see Sections 5-6 of this CA Privacy Statement for further information on how we share and sell your information, respectively.

(e) The right to no retaliation for opting out or exercising rights. California residents have a right of non-retaliation if they choose to exercise an employee right. If a California resident chooses to exercise any of these rights, we will not discriminate against the California resident in anyway.

(f) The right to limit use and disclosure of sensitive personal information. California residents have the right to request that we limit our use of their sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer of such services or goods.

(g) The right to opt-out of automated decision-making technology. If automated decision-making technology, including profiling, is used by us, California residents have a right to request meaningful information about the logic involved in automated decision-making technology and a description of the likely outcome of the process with respect to them.

5. Exercising California Employee Rights.

To exercise any of these rights, contact us at JBS.Compliance@jbssa.com or, if you are an employee of Pilgrim's Pride Corporation, Pilgrims.Compliance@pilgrims.com, or at the address in Section 7 of the Policy. **In connection with submitting a request, you must provide the following information: name, email, phone number, address (or state of residency) and you must state what type of request you are making.**

Only a California resident, or someone legally authorized to act on such California resident's behalf, may make a verifiable consumer request related to his or her personal information. In general, we have the right to require you to provide written permission granting authority to your representative and for your agent to verify their identity directly with us, and we may deny a request from your representative who does not submit proof of authorization as we request.

A California resident may only make a verifiable consumer request for access or data portability twice within a twelve (12) month period. The verifiable consumer request must provide sufficient information that allows us to reasonably verify the requestor is the person about whom we collected personal information or an authorized representative and describe the request with sufficient detail that allows us to properly understand, evaluate, and respond to it. We cannot respond to a request or provide personal information if we cannot verify the identity or authority to make the request.

We will: (a) confirm receipt of a request within ten (10) days following submission and provide information about how we will process the request; and (b) respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to an additional 45 days), we will you with written notice explaining the reason for the extended time period. We will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the twelve (12) month period preceding the request receipt date. If we deny a request, we will provide a response explaining the reasons we cannot comply with the request.

6. Sharing of California Employee Personal Information.

During the prior twelve (12) month period, we may have disclosed your personal information set forth in the categories identified in Section 1 of the Policy for a business purpose to the following categories of third parties our: (a) parent companies, affiliates, and/or joint venture partners; and (b) our security partners.

Additionally, during the prior twelve (12) month period, we may have shared your personal information set forth in the categories identified in Section 1 of the Policy to government agencies, law enforcement and our service providers.

7. Sale of California Employee Personal Information.

During the prior twelve (12) month period, we have not sold the Personal Information of a California employee.