TYSON GLOBAL PRIVACY NOTICE FOR JOB APPLICANTS

Maintaining the security of your data is a priority for Tyson Foods, Inc. and its subsidiaries, affiliates and related entities (collectively, "**Tyson**," "**we**" or "**us**"). Tyson is committed to being transparent about what data we collect about you and how we use it. This Privacy Notice applies to all current and former job applicants (collectively referred to as "**you**"). This Privacy Notice applies to Tyson's information practices for you to understand how personal data is collected, used, stored and disclosed. This Privacy Notice also describes your rights regarding the personal data we hold about you, including how you can exercise those rights.

This Privacy Notice may change from time to time. You should review this Privacy Notice periodically. We will bring any material changes to your attention by posting an updated version. Please note that the information practices regarding your use of Tyson's website, can be found at https://www.tysonfoods.com/privacy-policy.

WHO IS THE CONTROLLER OF YOUR PERSONAL DATA?

Under certain privacy laws, the "**Controller**" of your data is Tyson Foods, Inc. and the local Tyson entity to whom you have applied to for a role. We will only process your personal data according to this Privacy Notice unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive and processed for limited purposes.

WHAT IS PERSONAL DATA?

Personal data is information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, to an identified or identifiable living natural person or household. An 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or other factors that can identify an individual.

WHAT PERSONAL DATA DO WE COLLECT AND HOW DO WE USE IT?

Tyson only processes your personal data as the law allows or requires or according to this Privacy Notice.

We may collect the following categories of personal information about our job applicants. (Please note, not all categories may be collected about every individual):

- Personal Identifiers: such as name, phone, email, postal address, IP address
- Demographic Information: such as, gender, marital status, date of birth, age, military status
- Government Identifiers: such as driver's license numbers, visa information, state, province or national identification numbers, visa information or social security numbers, passport information

- Employment Information: such as experience and job history, compensation history, proof of work eligibility and drug screening
- Nominated References: detail on your nominated referees, such as their name, contact details, employer and job role
- Education Information: such as degree, school information, professional memberships and licenses as well as details included in your CV or resume
- Device Information: such as your interactivity with a job posting or website
- Security Information: such as CCTV footage from physical locations, data related to criminal convictions and offenses, traffic violations and vehicle accident history for applicants in the United States
- Health Information: information about your physical or mental condition
- Biometric Information: such as telephone recordings, facial recognition or fingerprint data
- Other Information you voluntarily provide throughout the process: such as through assessment centers or exercises and interviews

As a general rule, for job applicants during the recruitment process, we try not to collect or process any special categories of personal data that are sensitive under certain privacy laws ("**Sensitive Data**") and may receive special protection.

However, in some circumstances, we may need to collect, or request on a voluntary disclosure basis, some Sensitive Data for legitimate recruitment-related purposes: for example, information about your racial/ethnic origin, gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; information about your physical or mental condition to consider accommodations for the recruitment process and/or subsequent job role; data related to criminal convictions and offenses, traffic violation and accident history from job applicants located in the United States for the purposes of evaluating a job applicant's eligibility when such information is relevant to the position; surveillance footage, facial or fingerprint recognition or temperature checks from physical locations for access or entry purposes; or telephone recordings collected as part of the interview process to evaluate your employment eligibility. You may provide, on a voluntary basis, other Sensitive Data, during the recruitment process.

Where we request personal information and Sensitive Data from you, you can choose not to provide it to us. However, unless otherwise indicated, the information we request from you is required in order to enter into our contract of employment with you or in order to comply with our legal obligations. Failure to provide it prevents us from effectively entering into and administering a contractual relationship with you (including any related employment benefits) and/or complying, which may mean we are unable to offer you employment.

To comply with privacy laws of Canada, the European Union and the United Kingdom, we are providing the following additional details regarding our legal bases for processing your personal data.

Processing Purpose	Categories of Personal Information	Legal Basis for Processing
Evaluating eligibility of job applicants and making hiring decisions	Personal Identifiers Demographic Information Government Identifiers Education Information Employment Information Device Information Security Information Health Information Biometric Information Publicly available information	To meet our legitimate business interest to run our business effectively by assessing your application and suitability for employment including with respect to Sensitive Data to assess your working capacity You have consented to the use of your personal information Necessary for compliance with our legal obligations
Protecting the security and integrity of our business, processes and systems, including preventing unauthorized access to our computer and electronic communications systems;	Device Information	To meet our legitimate business interest to run our business effectively by securing our information, network, applications and systems

Processing Purpose	Categories of Personal Information	Legal Basis for Processing
preventing malicious software distribution and investigating any suspected security breaches		Necessary for compliance with our legal obligations
Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies)	Biometric Information Employment Information Personal Identifiers Security Information Government Identifiers Demographic Information Device Information	Necessary for compliance with our legal obligations to which we are subject and cooperate with regulators and law enforcement bodies To establish, exercise or defend legal claims
Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring	Personal Identifiers Security Information Biometric Information	Necessary for our own legitimate interests. For compliance with our legal obligations to which we are subject and cooperate with regulators and law enforcement bodies, as well as with employment laws and regulations With respect to Sensitive Data, to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law
Carrying out automated monitoring of IT communications and assess compliance with internal policies	Personal Identifiers Device Information Security Information	Necessary for our own legitimate interests to protect our systems and investigate any breaches of policy
Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations	Personal Identifiers Demographic Information Employment Information Device Information Security Information	Necessary for our own legitimate interests in effectively running our business and protecting our systems

HOW DO WE COLLECT YOUR PERSONAL DATA?

Generally, we collect any information you or a member of your household voluntarily share with us directly, through technology on Tyson-owned property or administered on Tyson's behalf, but we may also collect data from other sources. For example, we may collect the following:

- Human resources or employment information from another organization within our corporate family of companies;
- Certain background and other information from recruitment agencies, academic institutions, referees, credit reporting agencies or criminal record bureaus and other third parties during your recruitment;
- Information on your training and development from external training partners and information about your experience and impressions of Tyson through external survey providers;
- Information about your health, including your fitness to carry out work, from your healthcare provider, occupational health, other specialist medical advisor or Tyson's appointed medical expert;
- Information on accidents or incidents from Tyson's insurance brokers, insurers and their appointed agents, where they are involved;
- Information on tax payable from local tax authorities and Tyson's appointed payroll agents and tax/financial advisors;
- Information collected through Tyson's IT systems and other devices;
- Information about your entitlement to participate in, or receive payments or benefits under, any insurance or pension scheme provided by Tyson, from the relevant benefit provider or its appointed agent; or

- Information from publicly available sources (e.g. news sources and/or from social media platforms) in connection with any investigation or formal procedure concerning the same (for instance, an investigation of an allegation of conduct or breach if social media or IT policies)

To comply with certain United States state privacy laws, we are providing the following additional details regarding the categories of personal data collected within the last twelve (12) months and/or that we reasonably anticipate collecting moving forward.

Categories of Personal Information	Categories of Collection Sources	Processing Purpose
Personal Identifiers	Directly from you, such as individually provided contact information From our affiliates Non-affiliated third parties, such as witnesses in the event of an investigation or criminal record bureaus Service providers, such as website analytics service providers or recruitment agencies Through our IT systems and other devices Publicly available sources, as permitted by law, such as social media networks or news sources	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Government Identifiers	Directly from you, such as social security number or passport number Non-affiliated third parties, such as credit reporting agencies or government entities Service providers, such as recruitment agencies or background check providers	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies)
Demographic Information	Directly from you, such as date of birth, race or ethnic origin or marital status Non-affiliated third parties, such as government entities Service providers, such as recruitment agencies	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our

Categories of Personal Information	Categories of Collection Sources	Processing Purpose
		operational and technical functionality and complying with our legal obligations
Device Information	Directly from you Through our IT systems and other devices Service providers, such as IT security or monitoring providers or website analytics providers Cookies and similar technologies	Evaluating eligibility of job applicants and making hiring decisions Protecting the security and integrity of our business, processes and systems, including preventing unauthorized access to our computer and electronic communications systems; preventing malicious software distribution and investigating any suspected security breaches Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Security Information	Directly from you, such as a voluntary disclosure Through our IT systems and other devices, such as CCTV footage of entry to our facilities Non-affiliated third parties, such as criminal record bureaus Service providers, such as recruitment agencies or background check providers Publicly available sources, as permitted by law, such as social media networks or news sources	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Employment Information	Directly from you, such as information provided in your CV or resume Non-affiliated third parties, such as referrals Service providers, such as recruitment agencies	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality

Categories of Personal Information	Categories of Collection Sources	Processing Purpose
	Publicly available sources, as permitted by law, such as social media networks or news sources	control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Education Information	Directly from you, such as information provided in your CV or resume Non-affiliated third parties, such as referrals Service providers, such as recruitment agencies Publicly available sources, as permitted by law, such as social media networks or news sources	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Biometric Information	Directly from you, such as fingerprint recognition for facility access Through our IT systems and other devices	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Health Information	Directly from you, such as a voluntary disclosure Through our IT systems and other devices, such as temperature check upon entry at our facility Service providers, such as drug screening service providers	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations

Categories of Personal Information	Categories of Collection Sources	Processing Purpose
Publicly available information	Publicly available sources, as permitted by law, such as professional licensure information, social media networks, news sources	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations

HOW DO WE SHARE OR DISCLOSE YOUR PERSONAL DATA?

We may disclose your personal data to the following for the purposes set out in this Privacy Notice:

- Other members of our group of companies in order to administer human resources, staff member compensation and benefits at an international level on the human resources system, as well as for legitimate business purposes such as IT services/security, tax and accounting, and general business management.
- Third parties who provide services to us. For example, some personal data will be made available to:
    - Third party companies who provide us with recruiting support services;
    - Providers of our human resources platform;
    - Third parties who provide, support and maintain our IT and communications infrastructure (including for data storage purposes) and/or provide business continuity services;
    - Third parties who provide services in relation to applicant evaluation, onboarding and/or qualifications;
    - Third-party insurers, legal and professional advisers, or their representatives authorized on their behalf in connection with the advisory services they provide to us for legitimate business purposes and under a contractual prohibition of using the personal information for any other purpose.

We may also disclosure personal data to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant;
- In response to lawful requests by public authorities (including for tax, immigration, health and safety, national security or law enforcement purposes);
- As necessary to establish, manage, exercise, process or defend against potential, threatened or actual litigation or asserting our legal rights;
- Complying with our legal obligations;
- Preventing, investigating and detecting crime or fraud (including working with law enforcement agencies);
- Where necessary to protect the vital interests of another person;
- In connection with the sale, assignment or other transfer of all or part of our business; or
- With your consent.

We do not knowingly sell the personal information of minors under 18 years of age.

We may share within our companies and with certain third parties all categories of personal information, except for background and criminal information, biometric information, and government identifiers. We do not knowingly sell the personal information of minors under 17 years of age.

We may share and transfer your personal data for specific and definite purposes pursuant to the principles of lawfulness, fairness, necessity and good faith, and share and transfer the personal data to the extent necessary for the specific purposes you are informed of. If we share your personal data with recipients, where appropriate, we may use encryption, anonymization and other means as necessary and appropriate to ensure your personal data security. Before sharing or transferring your personal data, we will follow and adopt the applicable process and obligations required by the applicable law in respect of transfer of your personal data.

If Tyson is sold or disposed of as a going concern, whether by merger, reorganization, sale of assets or otherwise, or in the event of insolvency, bankruptcy or receivership, any and all personally identifiable information, including your account information may be one of the assets sold or merged in connection with that transaction. Information about you may also need to be disclosed in connection with a commercial transaction where Tyson is seeking financing, investment, support or funding. In such transaction, personal data will be subject to the promises made in any pre-existing privacy policy in effect when the information was obtained.

To comply with certain United States state and Filipino privacy laws, we are providing the following additional details regarding the categories of personal data collected within the last twelve (12) months and/or that we reasonably anticipate collecting moving forward.

Categories of Personal Information	Categories of Third Parties to Whom a Disclosure Was Made	Processing Purpose
Personal Identifiers	Other members of our group of companies Employees, officers, contractors Customers, in response to a contractual obligation or regulatory audit or investigation and under the cover of confidentiality Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Government Identifiers	Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies)

Categories of Personal Information	Categories of Third Parties to Whom a Disclosure Was Made	Processing Purpose
	Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	
Demographic Information	Other members of our group of companies Employees, officers, contractors Customers, in response to a contractual obligation or regulatory audit or investigation and under the cover of confidentiality Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Device Information	Other members of our group of companies Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions Protecting the security and integrity of our business, processes and systems, including preventing unauthorized access to our computer and electronic communications systems; preventing malicious software distribution and investigating any suspected security breaches Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational

Categories of Personal Information	Categories of Third Parties to Whom a Disclosure Was Made	Processing Purpose
		improvement, updating our operational and technical functionality and complying with our legal obligations
Security Information	Other members of our group of companies Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Carrying out automated monitoring of IT communications and assess compliance with internal policies Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Employment Information	Other members of our group of companies Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Education Information	Other members of our group of companies Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies)

Categories of Personal Information	Categories of Third Parties to Whom a Disclosure Was Made	Processing Purpose
	services are directly related to the processing of such information Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Biometric Information	Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations
Health Information	Employees, officers, contractors Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf whose services are directly related to the processing of such information Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions including with respect to Sensitive Data to assess your working capacity Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring including with respect to Sensitive Data to protect your vital interests or those of another person, or for reasons of substantial public interest for Sensitive Data in accordance with relevant law Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational

Categories of Personal Information	Categories of Third Parties to Whom a Disclosure Was Made	Processing Purpose
		improvement, updating our operational and technical functionality and complying with our legal obligations
Publicly available information	Other members of our group of companies Employees, officers, contractors Customers, upon request Third-party insurers, professional advisers, agents, third party service providers, suppliers, or subcontractors or their representatives authorized on their behalf Other organizations representing or acting on behalf of individuals who may request personal data to support a claim in relation to an incident or accident involving the individual Government agencies, authorities, regulators and law enforcement authorized to request personal data for lawful purposes or as otherwise required by law	Evaluating eligibility of job applicants and making hiring decisions Defending, managing or processing legal claims and complying with legal obligations; asserting our legal rights; preventing, investigating and detecting crime or fraud (including working with law enforcement agencies) Protecting the safety and wellbeing of employees and visitors to our sites; protecting our property and assets; and for equal opportunities monitoring Supporting internal operational and/or business purposes, such as strategic decisions, research and development, internal operations, projections, analytics, auditing and monitoring, detecting security incidents, improving our services, understanding our employee retention and attrition, quality control, identifying areas for operational improvement, updating our operational and technical functionality and complying with our legal obligations

IS MY PERSONAL DATA TRANSFERRED OUTSIDE OF MY HOME COUNTRY?

As we are a global company, your personal data may be processed by Tyson, its affiliates and other third parties described herein in countries other than the country of which you are a resident. Personal data may be sent to countries with different privacy laws than the country of your residence. Because the law in some of these countries does not provide the same level of protection, we implement appropriate safeguards and take measures to ensure adequate mechanisms are in place to protect your personal data in accordance with applicable data protection and privacy laws. We have data transfer agreements in place, which are considered appropriate safeguards implementing approved Standard Contractual Clauses to secure the transfer of your personal data to other jurisdictions. You can receive further information about the data transfer agreement by referencing the contact information below.

HOW DO WE PROTECT YOUR PERSONAL DATA?

We have implemented appropriate physical, technical, and organizational security measures designed to secure your personal data against accidental loss and unauthorized access, use, alteration, or disclosure. We also limit access to personal data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access.

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

Except as required by applicable law or regulation or as needed in connection with legal action or an investigation, we will only keep your personal data for as long as necessary to fulfill the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, we consider applicable legal requirements, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means. We specify the retention periods for your personal data in our data retention policy.

For job applicants, where you become a staff member at Tyson your personal data will form part of your employment record and your personal data will be kept in line with our retention periods for staff. Where you are unsuccessful, we will retain your personal data for a period of 12 months after confirmation that your application was unsuccessful unless you request that we delete your application. For applicants located in the United States, we may retain your information for an additional 24 months as required to evidence compliance with applicable employment laws.

HOW CAN I EXERCISE MY RIGHTS REGARDING MY PERSONAL DATA?

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes. Subject to limitations in applicable law, you may exercise specific rights you have to the personal data that we hold about you. Except as otherwise permitted by law, requests made regarding your personal information are free of charge.

Subject to the enforcement and limitations of applicable law, you generally may have a right to:

- Access, correct, update or request deletion of your personal data.
- Understand the existence of, authorization or basis for and circumstances surrounding the processing of your personal data.
- Object to processing of your personal data, ask us to restrict processing of your personal data or request portability of your personal data.
- Request information on automated processes where the personal data will or is likely to be made as the sole basis for any decision significantly affecting or will affect you.
- If we have collected and process your personal data with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of the processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.
- Complain to a data protection authority about our collection and use of your personal data. For more information, please contact your local data protection authority.

YOU MAY BE ENTITLED TO ADDITIONAL RIGHTS SPECIFIC TO THE LAWS OF YOUR JURISDICTION. YOU CAN FIND ADDITIONAL INFORMATION ABOUT YOUR PRIVACY RIGHTS FROM YOUR LOCAL CONSUMER OR PRIVACY PROTECTION GOVERNMENT AGENCY.

Additional Rights for Residents of United States

Subject to certain limitations under certain United States state laws and in addition to the disclosures and rights provided in this Privacy Notice, those state residents may request:

- A list of categories of personal data collected and used and whether that information is sold or shared. Any of the categories of personal information that we collect could be included in a sale to other companies, including those within our corporate family. If we have not sold your personal information, we will inform you of that fact.
- Request that we stop selling your personal information.

Additionally, and subject to certain limits under California law, California residents may request (i) a list of certain categories of personal data that we have disclosed to third parties for their direct marketing purposes during the immediately preceding calendar year, and (ii) the identity of those third parties. California residents may make one request per calendar year. Tyson does not share personal information for direct marketing purposes.

TO OPT-OUT OF THE SHARING OR SALE OF YOUR PERSONAL INFORMATION, PLEASE CLICK DO NOT SELL MY PERSONAL INFORMATION.

Please note that under applicable law, Tyson may in good faith reject, or deny requests that are duplicative, excessive and/or repetitive. If we deny your request, we will explain the reasons in our response. We will not discriminate against you for exercising these rights.

Version dated September 13, 2022

TO EXERCISE YOUR RIGHTS OR IF YOU HAVE ANY CONCERNS ABOUT TYSON'S PROCESSING OF YOUR PERSONAL DATA, PLEASE FIRST CONTACT YOUR HUMAN RESOURCES REPRESENTATIVE

CONTACT US AT E-MAIL PRIVACY@TYSON.COM AT OUR TOLL-FREE NUMBER +1-866-467-8688 AND ENTER SERVICE CODE 262# OR AT

Tyson Foods, Inc.
Privacy c/o Law Department
Mail Code CP004
2200 W. Don Tyson Parkway
Springdale, AR 72762-2020

IF YOU ARE A RESIDENT OF THE EUROPEAN UNION OR THE UNITED KINGDOM, YOU MAY ALSO CONTACT US AT

Legal Department
Tyson Foods Europe BV
Stadsplateau 7
3521 AZ Utrecht
Netherlands

ANY SUCH COMMUNICATION MUST BE IN WRITING.

Certain jurisdictions permit a consumer to designate an Authorized Agent to submit a disclosure or deletion request on behalf of the individual. To respond to a request from an Authorized Agent, we may:

- Request a copy of the written permission, such as a power of attorney or registration with the applicable government agency, granting the Authorized Agent to make such a request on the individual's behalf; and
- Verify the identity of the individual as described below.

Authorized agents use the same links described above to submit requests. Tyson may deny a request from an Authorized Agent that does not submit proof that they have been authorized by an individual to act on their behalf.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal data that we hold about you or make your requested changes. To verify your identity, we will generally match the identifying information provided in your request with the information we have on file about you. Depending on the sensitivity of the personal information requested, we may also utilize more stringent verification methods to verify your identity. We may ask you to provide other documentation to verify your identity. If this happens, we will reach out to you directly with this request. We may not be able to comply with your request if we are unable to confirm your identity or connect the information you submit in your request with personal information in our possession.

Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our data retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions. If you choose to exercise your rights, we will respond as required by law.

WHERE YOU ARE GIVEN THE OPTION TO SHARE YOUR PERSONAL DATA WITH US, YOU CAN ALWAYS CHOOSE NOT TO DO SO. IF YOU OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA, TYSON WILL RESPECT THAT CHOICE IN ACCORDANCE WITH ITS LEGAL OBLIGATIONS. THIS COULD MEAN THAT WE

ARE UNABLE TO PERFORM THE ACTIONS NECESSARY TO ACHIEVE THE PURPOSES OF PROCESSING DESCRIBED ABOVE, INCLUDING OFFERING AN EMPLOYMENT CONTRACT.

HOW CAN YOU CONTACT US?

We have appointed a Data Protection Officer to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal data or would like to request access to your personal data, please contact the Data Protection Officer at PRIVACY@TYSON.COM.

Version dated September 13, 2022