JOB APPLICANT PRIVACY POLICY

Contents

Scope

Belkorp Ag, LLC (the "**Company**," "**our**," "**us**," or "**we**") has developed this Privacy Policy out of respect for the privacy of our job applicants. This policy describes the Personal Information we collect, use, and disclose about individuals who apply for a position of employment. This is also to provide you with notice at or before the point at which we collect Personal Information from you informing you of what information we collect, how we use it, how long we retain it, and whether we sell it or share it for cross-context behavioral advertising purposes (*we don't by the way*). Personal Information is any information that could reasonably identify you.

This Privacy Policy applies only to your interaction with the Company in the capacity of a job applicant. It does not apply to other contexts, such as if you are hired for employment, in which case you would be provided with access to a privacy policy that covers information collected in the employment context, or if you visit our public-facing website or engage in transactions with the Company in other capacities (as a client, customer, or independent contractor), in which case the privacy policy https://www.belkorpag.com/privacy-policy on our website would apply to those interactions.

Consent to Use of AI Technology

Certain Company services and website features may be supported by third party vendors that utilize AI technology. When utilizing the text us or contact us features, our AI vendor(s) may record and transcribe information and may access the information in real-time and use the information for their own purposes, including to train their AI model. By using the text us or contact us features, you consent to the collection and analysis of any Personal Information provided. If you do not consent to such use and disclosure, please do NOT use these features. Please also review the information in the **Use of Automated Decisionmaking Technology (ADMT)** section of this policy.

Collection of Personal Information and Sensitive Personal Information

When you apply for a position or interact with us regarding potential job openings, we may collect Personal Information from you in a variety of different situations and using a variety of different methods, including, but not limited to, through our website, your mobile device, through email, written materials, in physical locations, and/or over the telephone. Generally, we will or may collect, and we have in the last 12 months collected, the following categories of Personal Information from or about job applicants. For each category of information, we identify the categories of third-parties, service providers, and contractors to whom we have disclosed the information in the last 12 months. The examples provided in each category are not intended to be an exhaustive list or an indication of all specific pieces of information we collect from or about you in each category, but rather the examples are to provide a meaningful understanding of the types of information that may be collected within each category.

Category	Identifiers
Examples	Name, alias, Social Security number, date of birth, driver's license or state identification card number, passport number, or Company ID number.
Disclosed in Last 12 Months To	• Government agencies • Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies • Social media platforms • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases • Our affiliated entities, including parent and subsidiary entities

Category	Contact Information
Examples	Home, postal or mailing address, email address, or home or cell phone number.
Disclosed in Last 12 Months To	• Government agencies • Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases • Our affiliated entities, including parent and subsidiary entities

Category	Pre-Hire Information
Examples	Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, information recorded in job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you, such as protected classifications.
Disclosed in Last 12 Months To	• Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies

	• Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases • Our affiliated entities, including parent and subsidiary entities

Category	**Professional or Employment-Related Information**
Examples	Information regarding prior job experience, positions held, and when permitted by applicable law your salary history or expectations.
Disclosed in Last 12 Months To	• Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases • Our affiliated entities, including parent and subsidiary entities

Category	**Education Information**
Examples	Information from resumes regarding educational history; information obtained from transcripts or records of degrees and vocational certifications obtained.
Disclosed in Last 12 Months To	• Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases • Our affiliated entities, including parent and subsidiary entities

Category	**Online Portal and/or Mobile App Access and Usage Information**
Examples	Where job applicant or candidate must create an account to apply for a job, the applicant's username and password, account history, usage history, file access logs, and any information submitted through the account.
Disclosed in Last 12 Months To	• Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases

Category	Inferences
Examples	Based on analysis of the Personal Information collected, we may develop inferences regarding job applicants' predispositions, behavior, attitudes, intelligence, abilities, and aptitudes for purposes of recruiting and hiring assessments and decisions.
Disclosed in Last 12 Months To	• Talent acquisition management systems and applicant tracking systems • Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process • Recruiting firms and/or staffing agencies • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases

What Sensitive Personal Information We Collect

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information we plan to collect:

- Identifiers (Social Security, driver's license, state identification card, or passport number)
- Online Portal and/or Mobile App Access and Usage Information (if required to create an account to apply for a job, your account log-in, in combination with any required security or access code, password, or credentials allowing access to the account)
- Medical and Health Information

Personal Information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the job applicant or from widely distributed media.
- Information made available by a person to whom the job applicant has disclosed the information if the job applicant has not restricted the information to a specific audience.
- De-identified or aggregated information.

Sources of Personal Information

We may collect your Personal Information from the following sources:

- You, the applicant, when you apply for a position of employment or voluntarily submit information
- Company systems, networks, software applications, and databases you log into or use in the course of applying for a position with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Surveillance cameras at our physical locations
- Credit and consumer reporting agencies

- HR support vendors
- Recruiting firms and/or staffing agencies
- Job platforms and career sites like Glassdoor, Indeed, LinkedIn, ZipRecruiter, etc.
- Personal references and former employers
- Schools, universities, or other educational institutions which you attended
- From friends, family, or colleagues who choose to email you jobs that they think you may be interested in from our application platform
- Our employees, contractors, vendors, suppliers, guests, visitors, other consumers, and customers based on your interactions with them (if any)

To Whom We Disclose Personal Information

We may disclose your Personal Information to the following categories of service providers, contractors, or third parties:

- Government agencies
- Talent acquisition management systems and applicant tracking systems
- Vendors providing services for purposes of our HRIS and management of job applicant data and recruiting process
- Recruiting firms and/or staffing agencies
- Credit and consumer reporting agencies
- Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants
- Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Social media platforms
- Our affiliated entities, including parent and subsidiary entities

Reasons Why We Collect, Use, Retain, and Disclose Personal Information

We may collect, use, and disclose your Personal Information for any of the following business purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to apply for a job with the Company, we will use that Personal Information in connection with your candidacy for employment.
2. To comply with local, state, and federal laws and regulations requiring employers to maintain certain records (such as immigration compliance records, accident or safety records, and tax records).
3. To evaluate, make, and communicate decisions regarding your job application and candidacy for employment.
4. To obtain and verify background checks, references, and employment history.
5. To communicate with you regarding your candidacy for employment.
6. To permit you to create a job applicant profile, which you can use for filling out future applications if you do not get the job you are applying for.

7. To keep your application on file even if you did not get the job applied for, in case there is another position for which we want to consider you as a candidate even if you do not formally apply.
8. To evaluate and improve our recruiting methods and strategies.
9. To engage in lawful monitoring of job applicant activities and communications when they are on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
10. To engage in corporate transactions requiring review or disclosure of job applicant records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
11. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company related to recruiting or processing of data from or about job applicants.
12. To improve job applicant experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
13. To protect against malicious or illegal activity and prosecute those responsible.
14. To prevent identity theft.
15. To verify and respond to consumer requests from job applicants under applicable consumer privacy laws.
16. To conduct risk assessments under applicable consumer privacy laws.
17. To conduct cybersecurity audits under applicable consumer privacy laws.
18. To conduct internal audits, compliance assessments, data analytics, and quality assurance activities.
19. To engage in strategic planning and operational efficiency.
20. To develop and improve our products and services based on your input, including developing, testing, and training our own custom software.

We do <u>NOT</u> and will not sell your Personal Information in exchange for monetary or other valuable consideration. We do not share your Personal Information for cross-context behavioral advertising.

We do <u>NOT</u> and will not use or disclose your Sensitive Personal Information for any purpose that gives rise to a right to limit the use or disclosure of your Sensitive Personal Information under the California Consumer Privacy Act (CCPA).

Retention of Personal Information

We will retain each category of Personal Information for as long as we continue to have a legal or business need to retain it consistent with the purposes for which the information was collected. Your Personal Information may be stored or maintained in a variety of different records, files, databases, and information systems some of which are controlled or managed by vendors. As a result, we are unable to predict at the point of collection of your information how long the information will be retained, as it depends on many factors. In deciding how long to retain each category of Personal Information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

Because the law prescribes minimum periods for retention of certain records, some records will be retained for at least the duration of the required period plus a certain number of years. Retention is often measured from occurrence of a triggering event but we may also measure the retention period from either (1) the date the record or data was collected, created, or last modified, (2) the date of the particular transaction to which the record or data pertains, or (3) another triggering event that is determined to be reasonable and appropriate based on the nature of the data and the legal/business needs for its continued use.

If the business purposes for collecting the Personal Information, and legal reasons for retaining the Personal Information, have both expired, we will purge the information in a secure manner.

Third-Party Vendors

We may use other companies and individuals to perform certain functions on our behalf. Such parties only have access to the Personal Information needed to perform these functions and may not use or store the information for any other purpose.

SMS Terms of Service

By subscribing to our SMS program, you agree to receive texts from the Company for purposes that include reminders about upcoming interviews, appointments, and processes. You voluntarily provide your phone number, and your phone number may be shared with our SMS service provider.

You can opt out at any time by replying **STOP** or get assistance by replying **HELP** or contacting us directly by phone (209) 821-1841.

Message frequency may vary. Message and data rates may apply. Consent is not a condition of employment.

Business Transfers

In the event we sell or transfer a particular portion of our business assets, applicant information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, applicant information may be transferred as part of the acquisition.

Compliance With Law and Safety

We may disclose specific Personal and/or Sensitive Personal Information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Passwords

The personal data record created through your registration for your Company or an associated vendor's account can only be accessed with the unique password associated with those records. To protect the integrity of the information contained in those records, you should not disclose or otherwise reveal your passwords to third parties.

Job Applicants Under the Age 16

We do not knowingly collect or disclose, let alone sell or share, the Personal Information of job applicants under 16 years of age.

How We Protect the Information That We Collect

The protection of the information that we collect about applicants is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We keep automatically collected data and voluntarily collected data separate at all times.
- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.

- We restrict access to private information to those who need such access in the course of their duties for us.

Use of Automated Decisionmaking Technology (ADMT)

We may make some significant decisions with what is considered an Automated Decisionmaking Technology. Applicants can appeal decisions to a human reviewer who has the authority to overturn the decision by utilizing the options outlined below.

Rights Under the CCPA

If you are a California resident, you have the following rights pursuant to the CCPA:

Right to Know	The right to request that we identify (1) the categories of Personal Information we have collected about you, (2) the categories of sources from which the Personal Information was collected, (3) the business or commercial purpose for collecting, selling, or sharing this information, (4) the categories of third parties with whom we disclose Personal Information, (5) the categories of Personal Information we sold or shared about you, and for each category identified, the categories of third parties to whom we sold or shared that particular category of Personal Information, and (6) the categories of Personal Information that we disclosed for a business purpose, and for each category identified, the categories of service providers or contractors to whom we disclosed that particular category of Personal Information.
Right to Access	The right to request that we provide you access to or disclose to you the specific pieces of Personal Information we have collected from or about you.
Right to Delete	The right to request that we delete Personal Information that we collected from you, subject to certain exceptions.
Right to Correct	The right to request that we correct inaccurate Personal Information (to the extent such an inaccuracy exists) that we maintain about you, and ensure any corrected data remains corrected.
Right to No Retaliation	The right to not be retaliated against for exercising privacy rights conferred by the CCPA, including when a consumer is an applicant to an educational program, a job applicant, a student, an employee, or an independent contractor.

Submitting a Consumer Request

You can submit any of the above types of consumer requests through any of the options below:

1. Submit an online request, **HERE**.
2. Call our privacy toll-free line at 800-457-7140.

How We Will Verify That it is Really You Submitting the Request:

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us.

Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within 45 calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our

written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly 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.

For a request to correct inaccurate Personal Information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the Personal Information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with a request, if applicable.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Consent to Terms and Conditions

By applying for a position with the Company or submitting any information for purposes of being considered for or inquiring about employment with the Company, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy

As our services evolve and we perceive the need or desirability of using information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check our website frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Privacy Policy, we will post the revised Privacy Policy and the revised effective date on this website. Please check back here periodically or contact us at the address listed at the end of this Privacy Policy.

Consumers With Disabilities

This policy is in a form that is accessible to consumers with disabilities.

Questions About the Policy

If you have any questions about this Privacy Policy, please contact us at hr@belkorpag.com or call (209) 340-0254.

EMPLOYEE PRIVACY POLICY

Contents

Scope of this Policy

Belkorp Ag, LLC (the "**Company,**" "**our**," or "**we**") has developed this Privacy Policy out of respect for the privacy of our employees and their family members, dependents, and beneficiaries. This Policy describes the Personal Information we collect, both online and offline, about employees who are employed with us and their family members, dependents, and beneficiaries. It explains the purposes for which we use and disclose Personal Information, how long we retain it, and whether we sell it or share it for cross-context behavioral advertising purposes (*we don't by the way*). Personal Information is any information that could reasonably identify you.

This Privacy Policy applies only to information collected, used, or disclosed by the Company in the employment context from or about employees and their family members, dependents, and beneficiaries. For purposes of this policy, "employment context" means any processing of Personal Information relating to the Company's personnel in connection with their work-related roles or activities. It does **not** apply to other contexts, such as if you visit our public-facing website or engage in transactions with the Company in other capacities (as a client or customer); interactions outside the employment context are subject to the privacy policy on our website.

Consent to Use of AI Technology

Certain Company services and website features may be supported by third-party vendors that utilize AI technology. When utilizing the text us or contact us features, our AI vendor(s) may record and transcribe information and may access the information in real-time and use the information for their own purposes, including to train their AI model. By using the text us or contact us features, you consent to the collection and analysis of any Personal Information provided. If you do not consent to such use and disclosure, please do NOT use the features.

Additionally, CoPilot is deployed across the Company's environment, which utilizes AI technology. When utilizing any CoPilot feature, Microsoft may record and transcribe information and may access the information in real-time and use the information for their own purposes, including to train their AI model. By using CoPilot's features, you consent to the collection and analysis of any Personal Information provided. If you do not consent to such use and disclosure, please do NOT use the features.

Finally, the Company utilizes certain John Deere applications that utilize AI technology. These applications may record and transcribe information and may access the information in real-time and use the information for their own purposes, including to train their AI model. By using the applications, you consent to the collection and analysis of any Personal Information provided.

Collection of Personal Information and Sensitive Personal Information

In the last 12 months, we have collected the following categories of Personal Information from or about employees and their family members, dependents, and beneficiaries. For each category of information, we identify below the categories of third parties, service providers, and contractors to whom we have disclosed the information in the

last 12 months. The examples provided in each category are not intended to be an exhaustive list or an indication of all specific pieces of information we collect from or about you in each category, but rather the examples are to provide you a meaningful understanding of the types of information that may be collected within each category.

Category	**Personal Identifiers**
Examples	Name, alias, Social Security number, date of birth, driver's license number, state identification card number, passport number, employee ID number, or professional license number, when provided to the Company.
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our human resources information system (HRIS) • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Communications providers • Social media platforms • Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister, or parent companies) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Contact Information**
Examples	Home, postal or mailing address, work and/or personal email address, or home or cell phone number, when provided to the Company.
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS

	• Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Communications providers • Social media platforms • Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • IT, cybersecurity, and privacy • Affiliated entities (subsidiaries, sister, or parent companies) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Account Information**
Examples	Username and password for access to Company accounts, databases, computers, and systems, and any required security or access code, password, or credentials allowing access to Company accounts.
Disclosed in Last 12 Months To	IT, cybersecurity, and privacy vendors and consultants

Category	**Protected Classifications**
Examples	Race, ethnicity, gender, disability, veteran or military status, when provided to the Company.
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister, or parent companies) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Physical Characteristics or Description**
Examples	Information on your driver's license (such as eye color, hair color, height, weight), as well as information collected to the extent relevant for workplace investigations or for enforcement of Company policies on appearance and grooming (such as tattoos, piercings).

Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister, or parent companies) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Financial Information**
Examples	Bank account number for direct deposit, credit or debit card number, or other financial account information, when provided to the Company.
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Internet, Network, and Computer Activity; Mobile Device Data**
Examples	Internet or other electronic network activity information related to usage of Company networks, servers, intranet, shared drives, or Company-issued computers and electronic devices, including system and file access logs, security clearance level, browsing history, search history, and usage history; data from employee devices identifying which devices access Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister companies, or parent company)

	• Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Geolocation Data**
Examples	IP address and/or GPS location (latitude & longitude) recorded on Company-issued computers, electronic devices, and vehicles, as well as timekeeping applications on cell phones that employees use to clock in and out and that log the geographic location at which each time entry was made.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Online Portal and Mobile App Access and Usage Information**
Examples	Username and password, account history, usage history, file access logs, and security clearance level from the Company's Online Portal or Mobile App.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Visual, Audio or Video Recordings**
Examples	Your image when recorded or captured in surveillance camera footage, videos collected in Company vehicles, pictures of employees taken in the workplace or at a Company function or event, or in pictures or video of employees posted on social media to which the Company or its managers have access or that are submitted to the Company by

	another employee or third party; recorded calls or meetings, such as recorded Zoom or Teams meetings.
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Communications providers • Social media platforms • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Pre-Hire Information**
Examples	Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Employment History
Examples	Information regarding prior job experience, positions held, names of prior supervisors, and, when permitted by applicable law, your salary history or expectations, when provided to the Company.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Education Information
Examples	Information from resumes regarding educational history; information in transcripts or records of degrees and vocational certifications obtained.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Driving Records
Examples	Information contained in your Department of Motor Vehicles record, including traffic violations, convictions, accident history, and departmental actions.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Affiliated entities (subsidiaries, sister companies, or parent company)

	• Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Professional or Employment-Related Information**
Examples	Information contained in your personnel file and in other employment documents and records, including information contained in the following types of records: new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury and safety records, performance evaluations and records, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, pension, retirement and 401(k) records, COBRA notifications, business expense and payroll records.
Disclosed in Last 12 Months To	• Financial institutions • Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Communications providers • Affiliated entities (subsidiaries, sister companies, or parent company) • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Facility & Systems Access Records**
Examples	Information identifying which employees accessed secure Company facilities, systems, networks, computers, and equipment, and at what times, using their keys, badges, fobs, login credentials, or other security access method.
Disclosed in Last 12 Months To	• Government agencies • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • IT, cybersecurity, and privacy vendors and consultants • Affiliated entities (subsidiaries, sister companies, or parent company)

	• Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Medical and Health Information**
Examples	Medical information contained in such documents as doctor's notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, ergonomic assessment and accommodation records, and correspondence with you and your medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as information in post-hire drug test results, and information related to symptoms, exposure, contact tracing, diagnosis, testing, or vaccination for infectious diseases (e.g., COVID-19), pandemics, or other public health emergency. This includes medical information and health benefits information for dependents and beneficiaries.
Disclosed in Last 12 Months To	• Government agencies • Benefits administrators and vendors, including third-party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors • Insurance carriers, administrators, and brokers • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	**Family Information**
Examples	Contact information for family members listed as emergency contacts; contact information for dependents and other dependent information, when provided to the Company.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Travel Information
Examples	Information regarding business travel, vacation, and personal travel plans, when provided to the Company.
Disclosed in Last 12 Months To	• Government agencies • Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Inferences
Examples	Based on analysis of the Personal Information collected through any means, we may develop inferences regarding employees' preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes for purposes of employment and management decisions related to staffing, assignments, responsibilities, team composition, hiring, promotion, demotion, and termination, among other things.
Disclosed in Last 12 Months To	• Employee tracking and talent management systems • Professional employer organizations, recruiting firms, and/or staffing agencies • Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS • Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators • Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Category	Contents of Personal Communications where the Company is not the intended recipient
Examples	If you use Company email, phones, computers, online chat applications (Slack, Teams, Zoom, etc.) or other Company systems for personal communications where the Company is not the intended recipient of the communication, the Company retains these communications in the ordinary course of managing its communication and computer systems and pursuant to the Company's data retention policy. Employees have no expectation of privacy with respect to any communications or data they send, receive, access or store on any Company computer or system, including any personal communications. The Company may monitor, access, review and use all such communications and data for lawful business purposes detailed below, including to manage and evaluate employee performance and make employment decisions.

Disclosed in Last 12 Months To	Not Disclosed

What Sensitive Personal Information We Collect

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information we plan to collect:

1. Personal Identifiers (Social Security number, driver's license, state identification card, or passport number)
2. Account Information (your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account)
3. Protected Classifications (racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, union membership, or sexual orientation)
4. Biometric Information (used for the purpose of uniquely identifying you)
5. Medical and Health Information
6. Geolocation Data (IP address and/or GPS location, latitude & longitude)
7. Contents of Personal Communications (contents of mail, email, and text messages where the Company is not the intended recipient)
8. Data of a Known Child (under 16 years of age)

Personal Information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the employee or from widely distributed media.
- Information made available by a person to whom the employee has disclosed the information if the employee has not restricted the information to a specific audience.
- De-identified or aggregated information.

Sources of Personal Information

We may collect your Personal Information from the following sources:

- You, the employee, when you voluntarily submit information for employment purposes
- Company-issued computers, electronic devices, and vehicles
- Company systems, networks, software applications, and databases you log into or use in the course of performing your job, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Surveillance cameras at our physical locations and in Company vehicles
- Drug testing and physical testing providers and vendors

- HR support vendors, including administrators of benefits, workers' compensation, unemployment claims, payroll, timekeeping, and expense management
- Social media platforms
- Recruiters and/or staffing agencies
- Personal references and former employers
- Our other employees, contractors, vendors, suppliers, guests, visitors, and customers, based on your interactions with them
- Affiliated entities (subsidiaries, sister, or parent companies)

To Whom We Disclose Personal Information

We may disclose your Personal Information to the following categories of service providers or contractors:

- Financial institutions
- Government agencies
- Promotional or other fulfilment vendors
- John Deere
- Benefits administrators and vendors, including third party administrators, 401K administrators, workers' compensation and unemployment administrators, and wellness vendors
- Insurance carriers, administrators, and brokers
- Employee tracking and talent management systems
- Professional employer organizations, recruiting firms, and/or staffing agencies
- Payroll processors, timekeeping vendors, and vendors providing services for purposes of our HRIS
- Consulting and investigation firms, including human resources consultants, safety consultants, and workplace investigators
- Communications providers/vendors (such as those who manage SMS text messaging or mailers)
- Social media platforms
- Our corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services)
- IT, cybersecurity, and privacy vendors, auditors, and consultants
- Auditors and financial consultants
- Affiliated entities (subsidiaries, sister, or parent companies)
- Company systems, networks, software applications, and databases you log into or use in your interaction with the Company, including from vendors the Company engages to manage or host such systems, networks, applications or databases.

Reasons Why We Collect, Use, Retain, and Disclose Personal Information

We plan to collect, use, and disclose your Personal Information for any of the following business purposes:

21. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to become an employee, we will use that Personal Information in connection with your employment.

22. To comply with local, state, and federal law and regulations including, but not limited to, requiring employers to maintain certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records).
23. To manage and process payroll and/or Company travel and expenses.
24. To validate an employee's identity for payroll and timekeeping purposes.
25. To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
26. To manage workers' compensation claims.
27. To administer, manage, and maintain group health insurance benefits, 401K and/or retirement plans, and other Company benefits and perks.
28. To manage employee performance of their job duties and/or employee conduct, including by engaging in lawful monitoring of employee activities and communications when they are on duty, on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
29. To monitor use of time off and ensure legal compliance regarding same.
30. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
31. To evaluate job applicants and candidates for employment or promotions.
32. To obtain and verify background checks on job applicants and employees and to verify employment references.
33. To evaluate, make, and communicate decisions regarding an employee's employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline.
34. To communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
35. To grant employees access to secure Company facilities and maintain information on who accessed the facility.
36. To track employee movement and activity throughout Company facilities and keep the facilities secure.
37. To provide employee training and other professional development opportunities such as coaching and mentoring.
38. To communicate with an employee's family or other contacts in case of emergency or other necessary circumstance.
39. To manage employee recognition programs.
40. To remain competitive in offering a variety of special discounts and benefits to employees.
41. To facilitate optional participation in Company-sponsored charity events.
42. To develop and improve our products and services based on your input and workplace activity, including developing, testing, and training our own custom software and artificial intelligence tools.
43. To engage in marketing efforts on behalf of the Company.
44. To track and record sales and other transactions with our customers.
45. To implement, monitor, and manage electronic security measures on Company internet and WiFi connections, computers, networks, devices, software applications or systems, as well as on employee devices that are used to access Company internet and WiFi connections, computers, networks, devices, software applications or systems.
46. To engage in corporate transactions requiring review or disclosure of employee records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
47. To comply with our contractual obligations.

48. To provide services to corporate customers who may request certain pieces of information about a Company employee (such as name, phone number, and headshot) to permit the employee access or security clearance to their facility in advance of the Company employee being dispatched to provide services at the customer's facility.
49. Infectious disease purposes (pandemic, outbreak, public health emergency, etc.)
50. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company.
51. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
52. To detect security incidents involving potentially unauthorized access to and/or disclosure of Personal Information or other confidential information, including proprietary or trade secret information and third-party information that the Company received under conditions of confidentiality or subject to privacy rights.
53. To protect against malicious or illegal activity and prosecute those responsible.
54. To prevent identity theft.
55. To verify and respond to consumer requests under applicable consumer privacy laws.
56. To conduct risk assessments under applicable consumer privacy laws.
57. To conduct cybersecurity audits under applicable consumer privacy laws.
58. To conduct internal audits, compliance assessments, data analytics, and quality assurance activities.
59. To engage in strategic planning and operational efficiency, including planning for appropriate staffing levels and resource management.

We do <u>NOT</u> and will not sell your Personal Information in exchange for monetary or other valuable consideration. We do not share your Personal Information for cross-context behavioral advertising.

We do <u>NOT</u> and will not use or disclose your Sensitive Personal Information for purposes that give rise to a right to limit the use and disclosure of your Sensitive Personal Information under the CCPA.

Retention of Personal Information

We will retain each category of Personal Information for as long as we continue to have a legal or business need to retain it consistent with the purposes for which the information was collected or the employment context. Your Personal Information may be stored or maintained in a variety of different records, files, databases, and information systems, some of which are controlled or managed by vendors. As a result, we are unable to predict at the point of collection of your information how long the information will be retained, as it depends on many factors. In deciding how long to retain each category of Personal Information that we collect, we consider many criteria, including, but not limited to, the business purposes for which the Personal Information was collected; relevant federal, state, and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

Because the law prescribes minimum periods for retention of certain employee records, some records will be retained for at least the duration of your employment plus a certain number of years. Retention is often measured

from occurrence of a triggering event, such as the end of your employment or relationship with us, but we may also measure the retention period from either (1) the date the record or data was collected, created, or last modified, (2) the date of the particular transaction to which the record or data pertains, or (3) another triggering event that is determined to be reasonable and appropriate based on the nature of the data and the legal/business needs for its continued use.

If the business purposes for collecting the Personal Information, and legal reasons for retaining the Personal Information, have both expired, we will purge the information in a secure manner.

Third-Party Vendors

We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail and payroll services. Such parties only have access to the Personal Information needed to perform these functions and may not use or store the information for any other purpose.

Business Transfers

In the event we sell or transfer a particular portion of our business assets, employee information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, employee information may be transferred as part of the acquisition.

Compliance With Law and Safety

We may disclose specific Personal and/or Sensitive Personal Information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Employees and Their Family Members, Dependents, and Beneficiaries Under the Age of 16

We do **not** knowingly sell or share the Personal Information of employees or any of their family members, dependents or beneficiaries under 16 years of age.

How We Protect the Information That We Collect

The protection of the information that we collect about employees is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We keep automatically collected data and voluntarily collected data separate at all times.
- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.

Rights Under the CCPA

If you are a California resident, you have the following rights pursuant to the CCPA:

1. Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of Personal Information we have collected, shared or sold about you, (2) the categories of sources from which the Personal Information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your Personal Information;

2. Right to Access. The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of Personal Information we have collected about you;

3. Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete Personal Information that we have collected from you, subject to certain exceptions;

4. Right to Correct. The right to request that we correct inaccurate Personal Information (to the extent such an inaccuracy exists) that we maintain about you, and ensure any corrected data remains corrected;

5. The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and

6. The right not to be retaliated against for exercising any of the above rights.

You Can Submit Any of the Above Types of Requests by Any of the Options Below:

1. Submit an online request on our website at https://app.termly.io/dsar/7ed93925-6fde-4dfb-9461-a84b568e9e21.

2. Call our privacy toll-free line at 800-457-7140.

How We Will Verify That it is Really You Submitting the Request:

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us.

Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly 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.

For a request to correct inaccurate Personal Information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the Personal Information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with a request, if applicable.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either: (a) execute a valid, verifiable, and notarized power of attorney; or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Consent to Terms and Conditions

By entering into an employment relationship with Belkorp Ag, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy

As our services evolve and we perceive the need or desirability of using Personal Information collected in other ways, we may, from time to time, amend this Privacy Policy. We encourage you to check the ADP Employee Platform frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Policy, we will post the revised Policy and the revised effective date on the ADP Employee Platform. Please check back here periodically or contact us at the address listed at the end of this Policy.

Individuals With Disabilities

This Policy is in a form that is or will be made accessible to individuals with disabilities.

Questions About the Policy

If you have any questions about this Privacy Policy, please contact us at HR@belkorpag.com or call (209) 340-0254.