Privacy Notice for Employees and Job Applicants

January 15, 2024

1. Introduction

Bell Techlogix, Inc. ("Bell Techlogix", "we" or "us") has issued this Privacy Notice (this "Notice") to describe how we handle Personal Data that we collect and process about our employees and job applicants (collectively referred to as "you") in the United States.

Please take the time to read and understand this Notice, which should be read in conjunction with our other Bell Techlogix policies and procedures and, with respect to employees, the employee handbook.

2. Types of Personal Data we collect

In the course of your employment at Bell Techlogix we may process Personal Data about you and your dependents, beneficiaries, and other individuals whose Personal Data has been provided to us.

We use the term "Personal Data" (also called "personal information" or "personally identifiable information" in the laws of some jurisdictions) to refer to information that reasonably identifies, relates to, describes, or can be associated with you. Data that has been de–identified, anonymized, or aggregated, or that otherwise cannot reasonably be related back to a specific person is not considered Personal Data. The precise definition of Personal Data may vary depending on your state of residence.

The types of Personal Data we may process include, but are not limited to:

Personal Data Category	Business Purpose
Identifiers, such as your full name, contact information, gender, date of birth, signature, Social Security number, driver's license or state identification numbers, and similar information for your dependents and beneficiaries.	• Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks. • Conduct employee onboarding • Maintain and administer payroll and employee benefit plans, including enrollment and claims handling. • Maintain personnel records and comply with record retention requirements. • Provide employees with human resources management services and employee data maintenance and support services. • Communicate with employees and their emergency contacts and plan beneficiaries.

	• Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of Bell Techlogix property, including information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to Bell Techlogix policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Bell Techlogix policy. • Respond to law enforcement requests and as required by applicable law or court order. • Exercise or defend the legal rights of Bell Techlogix and its wholly owned subsidiaries, employees, customers, contractors, vendors, and agents.
California Customer Records employment and personal information, such as your name, signature, Social Security number, physical characteristics or description, photograph, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, current employment, employment history, membership in professional organizations, licenses and certifications, bank account number, credit card number, debit card number, or any other financial,	• Same purposes as for identifiers category

medical or health insurance information	
Protected classification characteristics under California or federal law, such as age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, reproductive health decision making, military and veteran status, or genetic information (including familial genetic information).]	• Provide reasonable accommodation in compliance with the ADA. • Provide time off as required by law. • Provide and administer insurance coverage and benefits. • Design, implement, and promote Bell Techlogix' diversity, equity, inclusion & belonging initiatives. • Perform workforce analytics, data analytics, and benchmarking. • Conduct internal audits, grievances, and suspected violations of Bell Techlogix policy. • Exercise or defend the legal rights of Bell Techlogix and its wholly owned subsidiaries, employees, customers, contractors, vendors, and agents.
Biometric information, specifically, fingerprints	• Bell Techlogix Services, LLC is a wholly owned subsidiary of Bell Techlogix, Inc. Bell Techlogix Services, LLC performs work for clients who require security clearance. If an employee performs such work, they will be required to provide fingerprints as part of the process to obtain their security clearance. • Bell Techlogix employees employed in the Human Resources department may receive access to a restricted area at Bell Techlogix headquarters in which personnel records are stored. Access to the room is restricted by fingerprint access. • Bell Techlogix employees whose job functions require that they access servers in a restricted area at Bell Techlogix headquarters. Access to the server rooms is restricted by fingerprint access.

Internet or other similar network activity information, including all activity on Bell Techlogix information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords) and all activity on communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of Bell Techlogix-issued devices).	• Facilitate the efficient and secure use of Bell Techlogix information systems. • Ensure compliance with Bell Techlogix information systems policies and procedures. • Comply with applicable state and federal laws. • Prevent unauthorized access to, use, disclosure or removal of Bell Techlogix property, records, data, and information. • Enhance employee productivity. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Bell Techlogix policy. • Exercise or defend the legal rights of Bell Techlogix and its wholly owned subsidiaries, employees, customers, contractors, vendors, and agents.
Geolocation data, such as the time and physical location related to use of an internet website, application, or device	• Prevent unauthorized access, use, or loss of Bell Techlogix systems and property. • Ensure employee productivity and adherence to Bell Techlogix' policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Bell Techlogix' policy. • Exercise or defend the legal rights of Bell Techlogix and its wholly owned subsidiaries, employees, customers, contractors, vendors, and agents.
Surveillance data, such as call	• Comply with applicable state and federal laws, including on workplace health and safety.

monitoring and video surveillance.	• Prevent unauthorized access, use, or loss of Bell Techlogix property. • Improve customer service. • Exercise or defend the legal rights of Bell Techlogix and its wholly owned subsidiaries, employees, customers, contractors, vendors, and agents
Professional or employment-related information, such as employment application information (work history, academic and professional qualifications, educational records, references, and interview notes, background check, drug testing results, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information, leave of absence information including religious, military and family obligations, health data concerning employee and their family members.	• Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding. • Design and administer employee benefit plans and programs, including for leaves of absence. • Maintain personnel records and comply with record retention requirements. • Communicate with employees and their emergency contacts and plan beneficiaries. • Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of Bell Techlogix' property, including its information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to Bell Techlogix policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Bell Techlogix policy. • Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development.
Non-public education information, such as education records, degrees and vocational	• Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at Bell Techlogix

certifications obtained	
Inferences drawn from other personal information to create a profile or summary, for example, an individual's preferences, abilities, aptitudes, and characteristics.	• Engage in human capital analytics, including to identify correlations about individuals and job success, analyze data to improve retention and productivity, and analyze employee preferences to inform human resources policies and procedures. • Conduct applicant reference checks to assist in hiring decisions.

We do not sell Personal Data collected under this Notice and we do not share such Personal Data with third parties for cross-context behavioral advertising.

3. **Sources of Personal Data**

Usually, you will have provided the information we hold about you, but there may be situations where we collect Personal Data or Sensitive Personal Data from other sources. For example, we may collect the following:

a) Certain background and other information from recruitment agencies, academic institutions, background checking agencies and other third parties during your recruitment.
b) Certain information on your performance, conduct or other information relevant to formal internal procedures, from customers or other organizations you routinely work with.
c) Information on your training and development from external training partners and information about your experience and impressions of Bell Techlogix through external survey providers.
d) Information about your health, including your fitness to carry out work and/or any accommodations or adjustments to be considered from your doctor, or other specialist medical adviser.
e) Information on accidents or incidents from Bell Techlogix' insurance brokers, insurers, and their appointed agents, where they are involved.
f) Information on tax payable from local tax authorities and Bell Techlogix' appointed payroll agents and tax/financial advisers.
g) Information collected through Bell Techlogix' IT systems and other devices as set out above in Section 2.
h) Information about your entitlement to participate in, or receive payments or benefits under, any insurance or retirement plan provided by Bell Techlogix, from the relevant benefit provider or its appointed agent.
i) 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, for the investigation of an allegation that an employee member has breached our rules on social media use or conduct generally).
j) Indirectly from you by observing your actions on our website.

4. **Purposes for processing Personal Data**

(a) Recruitment purposes

If you are applying for another role at Bell Techlogix (and also, for example, if you are considering a transfer to another department or working for a different Bell Techlogix client), then we collect and use your Personal Data primarily to determine your qualifications for employment and to reach a hiring decision. This includes assessing your skills, qualifications, and background for a particular role, verifying your information, carrying out reference checks or background checks (where applicable) and to generally manage the hiring process and communicate with you about it. Bell Techlogix clients may require additional background check and drug screen requirements in addition to what you received when starting at Bell Techlogix. If this is the case, you will be made aware, and your prior consent obtained in accordance with applicable law.

If you are accepted for a role at Bell Techlogix, the information collected during the recruitment process will form part of your ongoing employment record.

If you are not successful, we may still keep your application for internal reporting and allow us to consider you for other suitable openings within Bell Techlogix in the future.

(b) Employment or work-related purposes

Once you become an employee at Bell Techlogix, we collect and use your Personal Data for the purpose of managing our employment relationship with you – for example, your employment records (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), and details of your spouse and dependents (for emergency contact and benefits purposes).

We process our employees' Personal Data through a human resources system called UKG ("HR System"), which provides tools that help us to administer HR and employee compensation and benefits, and which allows employees to manage their own Personal Data in some cases. This will involve transferring your Personal Data to our HR System provider's servers. Bell Techlogix may host these servers or utilize third party servers, but in either case will be responsible for ensuring the providers meet Bell Techlogix security requirements.

(c) The Bell Techlogix active directory

We maintain an active directory of employees which contains your professional contact details (such as your name, location, photo, job title and contact details). This information will be available to everyone in Bell Techlogix to facilitate cooperation, communication, and teamwork. Your photograph may also be required for your employee badge.

(d) Other legitimate business purposes

We may also collect and use Personal Data when it is necessary for other legitimate purposes, such as:

1. to help us conduct our business more effectively and efficiently – for example, for general HR resourcing, reporting or analytics, IT security/management, business continuity purposes, accounting purposes, or financial planning.
2. to investigate violations of law or breaches of our own internal policies and more generally to protect the rights and interests of Bell Techlogix, our employees, applicants and others. For instance, we may monitor your browsing or communications activity or location when using our devices or systems, if we suspect that you have been involved in phishing scams, fraudulent activity, or activities in competition with or inconsistent with your work for Bell Techlogix (for more information on such monitoring, refer to the End User Security Policy and Standard).
3. to help secure our networks and systems from unauthorized access, scams, and malicious code. For instance, we may monitor and review electronic mail communications sent or received using Bell Techlogix issued devices or accounts or stored on or using such a device or account. We may also monitor and record each website visit, each chat session, e-mail message, and each file transfer into and out of our systems and networks. Bell Techlogix may monitor this activity at any time, and, to the extent permitted by laws, users of our networks and systems should not expect privacy when using these systems and devices.

(e) Law-related and other purposes

We also may retain and use your Personal Data where we consider it necessary for complying with laws and regulations, including collecting and disclosing employee Personal Data as required by law (e.g. for tax, health and safety, anti-discrimination and other employment laws), under judicial authorization, to protect your vital interests (or those of another person), or to exercise or defend the legal rights of Bell Techlogix .

5. Who we share your Personal Data with

We allow access to Personal Data only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate business purpose or other lawful ground for accessing it. Third parties with access to Personal Data are contractually required to keep such Personal Data confidential and secure.

Transfers to third party service providers

In addition, we make certain Personal Data available to third parties who provide services to us. We do so in accordance with applicable data privacy laws.

For example, some of this information will be made available to:

a) our benefit/reward plans service providers (including retirement plans, for example OneAmerica, and medical insurance providers, for example Anthem).
b) service providers who provide us with payroll, tax and expense administration support services (for example, Concur).
c) providers of our HR platforms, for example UKG.

d) service providers who provide, support and maintain our IT, security, and communications infrastructure (including for data storage purposes) and/or provide business continuity services.
e) service providers who provide services in relation to employee training and/or qualifications (for example, Percipio) and employee surveys, for example the Great Place to Work Institute; and
f) auditors, advisors, legal representatives, and similar agents in connection with the advisory services they provide to us for legitimate business purposes and under a contractual or legal prohibition of using Personal Data for any other purpose.

Transfers to other third parties

We may also disclose Personal Data to third parties on other lawful grounds, including:

a) Where you have provided your consent.
b) 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, or government audit.
c) In response to lawful requests by public authorities (including for tax, immigration, health and safety, national security or law enforcement purposes).
d) As necessary to establish, exercise or defend against potential, threatened or actual legal claims.
e) Where necessary to protect your vital interests or those of another person; and/or
f) In connection with the sale, assignment, or other transfer of all or part of our business.
g) We do not sell the Personal Data we collect from and about you as described in Sections 2-4.

6. Data retention periods

Personal Data will be stored in accordance with applicable laws and kept as long as Bell Techlogix has an ongoing legitimate business need to carry out the purposes described in this Notice or as otherwise required by applicable law. Generally this means your Personal Data will be retained until the end or your employment, employment application, or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries, comply with regulatory obligations, or to deal with any legal matters (e.g. judicial or disciplinary actions), document the proper deductions during and on termination of your employment or work relationship (e.g. to tax authorities), or to provide you with applicable ongoing benefits, for example, COBRA.

7.Data Security

We have implemented measures designed to secure your Personal Data from accidental loss and from unauthorized access, use, alteration, and disclosure. The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain systems which store your Personal Data, you are responsible for keeping this password confidential. We ask you not to share your password with

anyone.

8. Updates to this Notice and Website Privacy Policy

This Notice may be updated periodically to reflect changes in our privacy practices. At a minimum, the Notice will be reviewed at least once annually and updated if needed. In such cases, we will indicate at the top of the policy the date on which it was most recently updated.

If we make a material change to how we treat your Personal Data (specifically, if we collect new Personal Data about you or use your Personal Data in ways not already established in this Notice), we will inform you by email to the email address specified in your job application and/or if you are an employee to your Bell Techlogix provided email address and/or publishing the updated version in UKG. We will also publish updated versions to our website and in UKG. We encourage you to check back periodically in UKG and our website in order to ensure you are aware of the most recent version of this Notice. We will obtain your consent to such material changes to the extent required by law.

Please see our separate Website Privacy Policy for additional information relating to our privacy practices for information collected via our website.

9. Additional Privacy Rights

Depending on the state from which you work, you may have additional state specific privacy rights. Please contact us using the below contact information if you have any questions. If you are a California resident, please see Section 11 below for additional rights.

10. How to Contact Us

Please provide enough information in your contact submission to permit us to respond. If you are a previous job applicant, please contact us by filling out the Contact Us Form on https://belltechlogix.com/contact-us/ and selecting "Human Resources" in the "Inquiry Type" drop down. You may also contact us via mail by sending an inquiry to:

Bell Techlogix, Inc.
Attn: Human Resources Dept
4400 W 96th Street
Indianapolis, IN 46268

If you are an employee, please contact us using the contact information provided to you in the employee handbook. Alternatively, you can raise any questions or concerns with your supervisor or the Chief Human Resources Officer.

11. California Residents

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months (the "right to know"). Once we receive your request and confirm your identity, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we disclosed your personal information for a business purpose (we do not sell your personal information), a list disclosing:
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.
- The specific pieces of personal information we collected about you (also called a data portability request).

Right to Delete

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions (the "right to delete"). Once we receive your request and confirm your identity, we will review your request to see if an exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Continue to provide employment related services to you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Exercise a right provided for by law.
4. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
5. Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us.
6. Comply with a legal obligation.
7. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify personal information not subject to one of these exceptions from our records and will direct our service providers to take similar action.

Exercising Your Rights to Know or Delete

To exercise your rights to know or delete described above, please submit a request by:

- Following the process in Section 10 How To Contact Us.

Only you, or someone legally authorized to act on your behalf, may make a request to know or delete related to your personal information.

You may only submit a request to know twice within a 12-month period. Your request to know or delete must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Please provide enough information in your request to permit us to respond. In order to verify your identity please provide the following in your request: (1) Current or former Bell Techlogix employees: Your full name and the email address associated with your profile; your preferred contact number; and your hire date; (2) Previous job applicants- Your full name and email address associated with your profile, your preferred contact number, the number of employment opportunities you have applied for with Bell Techlogix, as well as the job title associated with each application. For all requests, please indicate the specific California right (listed above) that you are exercising.

You do not need to create an account with us to submit a request to know or delete. However, we do consider requests made through an employee password protected account (for example, requests sent through a Bell Techlogix provided email account or Teams account) sufficiently verified when the request relates to personal information associated with that specific account. If the request comes from an account not provided by Bell Techlogix, then we will verify you by matching you with information we have on record for you (for example by calling you at the phone number we have on record for you and/or emailing you at the email address we have on record for you).

We will only use personal information provided in the request to verify the requestor's identity or authority to make it.

Response Timing and Format

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10-day timeframe, please contact us using the information above in Section 10.

We endeavor to substantively respond to a verifiable request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period in writing.

If you have an employee account (for example a Bell Techlogix provided email account) with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer 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.

Personal Information Sales Opt-Out and Opt-In Rights

We do not sell your personal information; therefore, we do not provide you with a mechanism for opting out.

Right to Non-Discrimination

Bell Techlogix does not discriminate against those who exercise their rights under the CCPA.