



CommandLink Worker and Applicant Privacy Notice

Effective Date: January 1, 2026

CommandLink, LLC must retain and process information about you for purposes of our working relationship. We use your information to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately. We must do this during the application process, while you are working for us, at the time when you stop doing work for us and after you have left CommandLink.

This Privacy Notice is provided at or before the time personal data is collected. It explains how we collect, use, disclose, retain and safeguard personal data, the legal bases for processing, whether provision of data is mandatory and the rights available to you under applicable U.S. federal and state laws and international data protection laws.

1. Scope

This Privacy Notice applies to all current, former and prospective job applicants, employees, interns, contractors or workers whose personal data is collected by CommandLink for employment or work-related purposes.

Workers should have no expectation of privacy when using company systems or devices, except where and to the extent required by applicable law. This includes lawful electronic monitoring of communications, devices, networks and facilities for business, security, compliance and safety purposes.

2. Personal Data Collected

We have collected and processed, or may collect and process the following categories of personal data:

- Personally Identifiable Information: Name, date of birth, gender, nationality, physical characteristics, signature, government-issued identification numbers and similar identifiers.
- Contact Details: Home address, email addresses, phone numbers and physical location.
- Employment, Professional and Education Data: Job title, employment history, performance data, disciplinary records, compensation, employee ID numbers and education records.
- Health and Medical Information: Medical and insurance information, disability and occupational health data, dependent or beneficiary information and COVID-19-related information where permitted by law.
- Biometric Information: Fingerprints, facial images, voiceprints or other biometric identifiers where permitted by law.
- Financial Data: Bank account information, payroll, tax and benefits data.
- IT, Security and Monitoring Data: Network activity, system usage, access logs, emails, messaging, texts, browsing activity, geolocation data, device identifiers, CCTV footage and security alerts.
- Background Check Data: Criminal history, credit checks and references where permitted by law.
- Sensitive Personal Information: Race, ethnicity, citizenship, marital status, sexual orientation, religious beliefs (where voluntarily provided) and veteran or military status.
- Communication Records: Call logs, text metadata, voicemail and recorded communications.
- Third-Party Information: Personal data relating to dependents, beneficiaries, emergency contacts or other individuals provided by you.

Certain personal data is required by law or contract. Failure to provide required information may affect employment, compensation, benefits or continued engagement.

3. Purposes of Processing

Personal data is collected and processed for purposes including:

- Recruitment, hiring, onboarding and training
- Employment and contractor administration
- Payroll, compensation and benefits administration

- Performance management and workforce planning
- Health, safety and security
- IT systems management and monitoring
- Compliance with legal and regulatory obligations
- Investigations, audits and legal proceedings
- Separation and offboarding management

Sensitive personal information is used only for purposes reasonably necessary and proportionate to these activities or as otherwise permitted by law.

4. Legal Basis for Processing

Where applicable, processing is based on performance of a contract, compliance with legal obligations, legitimate business interests, or consent where required by law. Where processing is based on consent, you may withdraw consent at any time.

5. Privacy Rights

Depending on your location, you may have rights to:

- Access your personal data
- Correct inaccurate data
- Request deletion of data
- Restrict or object to processing
- Limit use of sensitive personal information
- Receive a portable copy of your data
- Withdraw consent
- Appeal denied requests where applicable
- Submit a complaint with a supervisory authority
- Not be retaliated against for exercising privacy rights

Requests may require identity verification.

6. Data Sharing and Transfers

Personal data may be shared with government authorities, payroll and benefits providers, professional advisors, IT service providers and transaction counterparties when necessary. CommandLink does not sell personal data or share it for cross-context behavioral advertising. International transfers are conducted using lawful safeguards such as Standard Contractual Clauses.

7. Data Retention

Personal data is retained only for as long as reasonably necessary to fulfill the purposes described in this Privacy Notice, including employment, legal, regulatory, contractual, security and business obligations. Retention periods vary depending on the type of data, the nature of the relationship and applicable legal requirements. Data is securely deleted or anonymized when no longer required.

8. Data Security

Appropriate technical and organizational measures are used to protect personal data from unauthorized access, loss, misuse or disclosure.

9. Amendments

This Privacy Notice may be amended from time to time. Material changes will be communicated as required by law.

10. Contact Information

Legal Department / Data Protection Officer
CommandLink, LLC
Privacy@CommandLink.com
PO Box 4085
Portsmouth, NH 03082