PRIVACY NOTICE TO CALIFORNIA EMPLOYEES REGARDING THE COLLECTION OF PERSONAL DATA

Effective August 2024

Download | Accessible Version

DUAL North America, Inc. and its subsidiaries and affiliates, ("the Company") are committed to protecting the privacy and security of personal information of its current and former employees, job applicants, temporary employees, and contractors (collectively, "Personnel"). The Company therefore provides this DUAL North America, Inc. Privacy Notice ("Privacy Notice") to provide information to California Personnel – and other individuals whose Personal Data is collected for human resources purposes (such as qualified dependents) – regarding how the Company collects and uses Personnel's Personal Data in connection with their employment and other relationship with the Company. In this Privacy Notice, "Personal Data" means data relating to identified or identifiable individuals and households.

The Company does not sell, share, or otherwise disclose this personal information for monetary consideration or a business purpose to any third parties except the Company may share the categories of information listed below with vendors the Company uses to perform necessary functions to facilitate employee payment, benefits, health and safety, and insurance.

The Company is committed to complying with the California Consumer Privacy Act (CCPA"), as amended, and all data privacy and laws in the jurisdictions in which it employs employees. Employees, emergency contacts, and beneficiaries may access this notice in an alternative format by contacting hr@dualinsurance.com.

WHAT IS THE COMPANY'S PRIVACY POLICY?

The Company's consumer Privacy Policy ("Consumer Privacy Policy" available at https://www.dualna.com/dual-privacy-policy) describes how the Company collects, uses, and protects the Personal Data of individuals who use the Company's website and other online services. The Company's Consumer Privacy Policy will apply to the extent Personnel use any products or services subject to the Consumer Privacy Policy.

WHAT IS THE COMPANY'S CONTACT INFORMATION?

If you have any questions or concerns regarding this Privacy Notice, the Company's Privacy Policy, or the collection of your personal information, please contact legal@dualinsurance.com.

See below for information relating to how to submit requests to exercise Personnel's rights in the Personal Data the Company processes.

WHAT CATEGORIES OF EMPLOYEE INFORMATION DO WE COLLECT AND HOW DO THE COMPANY USES THIS INFORMATION?

This chart describes the categories of Personal Data that the Company may collect in connection with its employment and contractual work relationships. Note: all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of Personal Data & Representative Data Elements	**Common Purposes for Collecting & Sharing**
Contact Data • Honorifics and titles, preferred form of address • Mailing address • Email address • Telephone number • Mobile number	The Company uses your Contact Data to communicate with Personnel by mail, email, telephone, or text about their employment, including sending them work schedule information, compensation and benefits communications, and other company information. Contact Data is also used to help the Company identify Personnel and personalize the Company's communications, such as by using Personnel's preferred name.
Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Employee ID number • Company account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	The Company uses Personnel's Identity Data to identify Personnel in the Company's human resources records and systems, to communicate with Personnel (often using their Contact Data) and to facilitate the Company's relationship with Personnel, for internal record-keeping and reporting (including for data matching and analytics), to track Personnel's use of company programs and assets, and for most processing purposes described in this Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security/national insurance number • Driver's license information • Passport information • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number*)	The Company uses Personnel's Government ID Data to identify Personnel and to maintain the integrity of the Company's human resources records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks (subject to applicable law), enable the Company to administer payroll and benefits programs and comply with applicable laws (such as reporting compensation to government agencies as required by law), as well as for security and risk management (such as collecting driver's license data for Personnel who operate company vehicles, professional license verification, fraud prevention and similar purposes).

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
	The Company may also use Government ID data for other customer Business Purposes, such as collecting passport data and secure flight information for Personnel who travel as part of their job duties.
Biographical Data • Resume or CV • Application and screening questionnaires • Data from information publicly available on the Internet • Education and degree information • Employment or other work history • Professional licenses, certifications, and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests, and hobbies • Professional goals and interests • Criminal records	The Company uses Biographical Data to help the Company understand its Personnel and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between each individual's background and relevant job functions. The Company also uses Biographical Data to foster a creative, diverse workforce, for recruiting, for coaching, and to guide its decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, and Reporting Information • Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	The Company uses Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g., onboarding, maintenance, evaluations, performance management, investigations, etc.).
Financial Data • Bank account number and details • Company-issued payment card information, including transaction records • Tax-related information	The Company uses Personnel's Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, for tax withholding purposes, and for security and fraud prevention.

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
Health Data • Medical information for accommodation of disabilities • Medical information for leave and absence management, and emergency preparedness programs • Vaccination status • Wellness program participation • Information pertaining to enrollment and utilization of health and disability insurance programs	The Company uses Personnel's Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics related to the Company's human resources functions, staffing needs, and other Business Purposes. In response to a pandemic, the Company may implement health and other screening procedures, vaccination requirements, vaccination tracking, and other measures to reduce the possibility of transmission to Personnel and to comply with applicable public health orders and guidance. The Company may use and may need to share this data to carry out contact tracing, implement and enforce workplace safety rules, and for public safety reasons and compliance obligations.
Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet search and browsing history, metadata and other technically-generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	The Company uses Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. The Company may also use this information to evaluate compliance with Company policies. For example, the Company may monitor employee activity on Teams, email traffic, and work activity on some electronic systems to verify work hours and attendance records. The Company's service providers may use this information to operate systems and services on the Company's behalf, and in connection with service analysis, improvement, or other similar purposes related to the Company's business and human resources functions.
Audio/Visual Data • Photographs • Video images and videoconference records • Call center recordings and call monitoring records • Voicemails	The Company may use Audio/Visual Data for general relationship purposes, such as call recordings used for training, coaching, or quality control.
Inference Data • Performance reviews	The Company uses Inference Data to help tailor professional development programs and to determine suitability for advancement or other positions. The

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
• Results of tests related to interests and aptitudes	Company may also analyze and aggregate data for workforce planning. Certain Inference Data may be collected in connection with information security functions (e.g., patterns of usage and cybersecurity risk).
Compliance and Demographic Data • Employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA, etc. • Occupational safety records and workers' compensation program records • Records relating to internal investigations • Records of privacy and security incidents involving human resources records, including any security breach notifications	The Company uses Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, and as needed for litigation and defense of claims.
Protected Category Data Characteristics of protected classifications under state or federal law, e.g. race, national origin, religion, gender, disability, marital status, veteran status, sexual orientation, or gender identity	The Company uses Protected Category Data as needed to facilitate the employment relationship or other relationship, for compliance and legal reporting obligations, to evaluate the diversity of our Personnel and the success of our diversity and inclusion efforts, and as needed for litigation and defense of claims.

WHAT ARE THE SOURCES OF PERSONAL DATA?

The Company collects Personal Data from various sources, which vary depending on the context in which the Company processes that Personal Data.

- **Data Personnel provide to the Company** – The Company will receive Personnel's Personal Data when Personnel provide them to the Company, apply for a job, complete forms, provide Personal Data via Workday, or otherwise direct information to the Company.
- **Data from a third party** – The Company will receive Personnel's Personal Data from third parties such as recruiters, credit reporting agencies, or employment screening providers.
- **Data from publicly available sources** – The Company may collect data that is publicly available on the Internet (e.g. through a Google search of a candidate's name).

- **Data the Company automatically collects**– The Company may also collect information about or generated by any device Personnel have used to access internal IT services, applications, and networks.
- **Data the Company receives from Service Providers** – The Company receives information from service providers performing services on our behalf.
- **Data the Company creates or infer** – The Company (or third parties operating on the Company's behalf) create and infer Personal Data such as Inference Data based on its observations or analysis of other Personal Data processed under this Privacy Notice, and the Company may correlate this data with other data the Company processes about Personnel. The Company may combine Personal Data about Personnel that it receives from Personnel and from third parties. We do not infer Sensitive Personal Data.

HOW DOES THE COMPANY DISCLOSE PERSONAL DATA?

The Company generally process Personal Data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

Categories of Internal Recipients

The Personal Data identified below collected from the Company's Personnel may be disclosed to the following categories of recipients in relevant contexts:

- **Personnel of Human Resources Departments** – All Personal Data relating to human resources and Recruitment.
- **Personnel of Finance Departments** – Personal Data to the extent related to payroll, compensation, expense reimbursements, etc.
- **Supervisors and Managers –** Elements of Personal Data, to the extent permitted in the jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment or contractual relationship, conduct reviews, handle compliance obligations, and similar matters.
- **Department Managers searching for new employees or contractors** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.
- **IT Administrators** of the Company and/or third parties who support the management and administration of human resources processes may receive Personal Data as necessary for providing relevant IT related support services (for example, conducting IT security measures and IT support services)**.**
- **Peers and colleagues –** Elements of Personal Data in connection with company address books, intracompany and interpersonal communications, and other contexts relevant to the day-to-day operation of company business.

Categories of External Recipients

The Company may provide Personal Data to external third parties as described below. The specific information disclosed may vary depending on context, but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and The Company. The Company generally provide information to:

- The Company's affiliates.
- Service providers, vendors, and similar data processors that process Personal Data on the Company's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, background checks, etc.) or that provide other services for Personnel or for the Company.
- To prospective seller or buyer of such business or assets in the event the Company sells or buys any business or assets.
- To future Company affiliated entities, if the Company or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its employees and contractors may be one of the transferred assets.
- To Personnel's employment references, to inform them that the Personnel applied with the Company as part of its recruiting process.
- To future prospective employers seeking to confirm Personnel's relationship with the Company.
- To government agencies or departments, or similar parties in connection with employment-related matters.
- To any public authority in relation to national security or law enforcement requests, if the Company is required to disclose Personal Data in response to lawful requests by a public authority.
- To any other appropriate third party, if the Company is under a duty to disclose or share Personnel's Personal Data to comply with any legal obligation or to protect the rights, property, health, or safety of the Company, Personnel, customers, or others.

Locations of Recipients

The Company and The Company affiliates are located in the United States. Any Personal Data collected under this Privacy Notice will likely be processed in the United States.

The Company collects this information to contact the Employee's designated emergency contact persons in the event of an emergency.

WHAT ARE THE PURPOSES OF COLLECTING, USING, AND DISCLOSING PERSONAL DATA?

The Company collects Personal Data about its prospective, current, and former Personnel and other individuals as appropriate in the context of an employment or contractual work relationship (such as dependents) for various general human resources and business purposes, as described below. The Company does not sell to or "share" (as defined in the California Consumer Privacy Act, as

amended) Personal Data with third parties in exchange for monetary consideration or for advertising purposes.

General Human Resources Purposes

The Company collects Personal Data about its prospective, current, and former Personnel and other individuals as appropriate in the context of an employment or contractual work relationship, including for recruitment and IT/technical support services, and as needed for using internal software, networks and devices. The categories of Personal Data the Company processes, along with representative data elements, are listed in the chart below. The Company may not collect from Personnel or process all of the Personal Data identified below, depending on Personnel's position or the nature of Personnel's relationship with the Company.

The Company generally processes Personal Data for the following purposes:

Personal Data pertaining to ***prospective*** Personnel may be processed for:	• Recruitment and staffing, including evaluation of skills and job placement. • Hiring decisions, including negotiation of compensation, benefits, relocation packages, etc. • Risk management, including reference and other background checks. • The Company's Business Purposes (defined below).
Personal Data pertaining to ***current*** Personnel may be processed for:	• Staffing and job placement, including scheduling and absence management. • Verification of eligibility to work and compliance with immigration laws, rules and regulations. • Administration of compensation, employee recognition, insurance and benefits programs. • Time and attendance tracking, company vehicle use, expense reimbursement, other workplace administration and facilitating relationships within the Company. • Technology support uses, such as managing our computers and other assets, providing email and other tools to Company workers. • EEO/Affirmative Action programs. • Internal and external directories of Personnel. • Health and wellness programs. • Reasonable accommodations. • Occupational health and safety programs (including drug and alcohol testing, required injury and illness reporting, disaster recovery and business continuity planning, and workers' compensation management).

	• Health and safety requirements imposed by the Company, government authorities, or others, depending on the location of employment, engagement or travel (e.g. vaccination status or health screening). • Talent and performance development, skills management and training, performance reviews, employee feedback surveys, and recognition and reward programs. • Human resources support services, such as responding to inquiries, and providing information and assistance. • Employee relations, such as implementing and administering Human resources policies, investigations, and resolving disputes or concerns that you may raise. • Risk management and loss prevention, including employee and premises monitoring. • Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken, such as making adjustments. • Managing statutory leave programs such as family and parental leave. • Succession planning and adjustments for restructuring. • As requested by individuals, including to verify employment and income verifications (e.g., for mortgage applications). • The Company's Business Purposes (defined below).
Personal Data pertaining to ***former*** Personnel may be processed for:	• Re-employment. • Administration of compensation, insurance and benefits programs. • Expense reimbursements. • For archival and recordkeeping purposes. • Responding to claims for unemployment benefits and other government inquiries. • As requested by individuals, including employment and income verifications (e.g., for mortgage applications). • EEO/Affirmative Action programs. • The Company's Business Purposes (defined below).
Personal Data pertaining to individuals whose information is provided to the Company in the course of human resources management (such as information pertaining to employees'	• Administration of compensation, insurance and benefit programs. • Workplace administration. • To comply with child support orders or garnishments. • To maintain emergency contact lists and similar records. • The Company's Business Purposes (defined below).

family members, beneficiaries, dependents, emergency contacts, etc.) may be processed for:

Business Purposes

"Business Purposes" means the following purposes for which Personal Data may be collected, used and shared:

- Maintaining comprehensive and up-to-date Personnel records.
- Establishing, managing, or terminating the employment or other working relationship.
- Maintaining a safe and respectful workplace and improving Personnel satisfaction and performance.
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials.
- Security, safety, loss prevention, information security, and cybersecurity.
- Legal and regulatory compliance, including without limitation all uses and disclosures of Personal Data that are required by court orders and applicable laws, regulations, orders and ordinances, and for compliance with legally-mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics reporting system, and other processing in connection with the establishment and defense of legal claims.
- Corporate audit, analysis, and consolidated reporting.
- To enforce the Company's contracts and to protect the Company, its workers, its customers and their employees, and the public against injury, theft, legal liability, fraud or abuse, to people or property.
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research, or analytics.
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the operations, analysis, upgrade, enhancement, development, or improvement internal IT or other services, operations, and similar matters.
- As needed to facilitate corporate governance.

HOW IS DATA ADMINISTRATION HANDLED?

Security

The Company requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in the Company's various security policies. Company staff must follow the security procedures set out in applicable security policies at all times.

Retention and Disposal

The Company intends to retain Personal Data or Sensitive Personal Data (as defined above) for no longer than is reasonably necessary and proportionate to achieve the legitimate business purpose for which it was collected or to satisfy a legal requirement. What is necessary may vary depending on the context and purpose of processing. The Company generally considers the following factors when it determines how long to retain data (without limitation):

- Retention periods established or necessary under applicable law;
- Industry and human resources best practices;
- Whether the purpose of processing is reasonably likely to justify further processing;
- Risks to individual privacy in continued processing;
- Applicable data protection impact assessments;
- IT systems design considerations/limitations; and
- The costs associated continued processing, retention, and deletion.

Company staff must follow any applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with applicable company policies, including the Company Data Retention Policy. Personal Data shall not be further processed in a manner that is incompatible with these purposes.

WHAT ARE PERSONNEL'S RIGHTS AND CHOICES?

Personnel Rights, Including Personnel California Privacy Rights

Under the California Consumer Privacy Act ("**CCPA**") and other comprehensive state privacy laws, Personnel may have the following rights, subject to Personnel's submission of an appropriately verified request (see below for verification requirements):

Right to Know	Personnel may request any of following, for the 12-month period preceding the request: (1) the categories of Personal Data the Company collected about that Personnel, or that the Company sold, or disclosed for a commercial purpose; (2) the categories of sources from which that Personnel's Personal Data was collected; (3) the business or commercial purpose for which the Company collected, sold or shared that Personnel's Personal Data; (4) the categories of third parties to whom the Company sold or shared that Personnel's Personal Data, or disclosed it for a business purpose; and (5) the specific pieces of Personal Data the Company collected about that Personnel.
Right to Delete	Personnel have the right to delete certain Personal Data that the Company holds about that Personnel, subject to exceptions under applicable law.
Right to Correct	Personnel have the right to correct certain Personal Data that the Company holds about that Personnel, subject to exceptions under applicable law.
Right of Non-retaliation	Personnel have the right to not to receive discriminatory treatment as a result of that Personnel's exercise of rights conferred by the CCPA.

Direct Marketing	Personnel may request a list of Personal Data the Company disclosed about that Personnel to third parties for direct marketing purposes during the preceding calendar year, if applicable.
Minors'	To the extent the Company has actual knowledge that the Company collects or maintains Personal Data of a minor under age 16, those minors between the age of 13 and 16 must opt-in to any sharing of personal information (as defined under CCPA), and minors under the age of 13 must have a parent consent to sharing of personal information (as defined under CCPA). All minors have the right to opt-out later at any time. Minors under age 13 may have other rights under the Children's Online Privacy Protection Act ("COPPA").

Submission of Requests

Current Company employees and contractors can review and update much of their Personal Data via Workday.

Current Company employees can send an email to hr@dualinsurance.com to submit requests to review and update their Personal Data and to exercise their rights in Personal Data subject to this Privacy Notice, to the extent those rights are available under applicable law. Current Company employee may also contact the Human Resources Office for assistance. Contractors, applicants, former employee, beneficiaries, dependents, and family members, may contact legal@dualinsurance.com or at (855) 378-8203. For all other questions or comments about this Privacy Notice or the Company's privacy practices, please contact hr@dualinsurance.com or at (855) 378-8203.

Verification of Requests

Requests to receive a copy of Personal Data, and requests to delete or correct Personal Data, must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of the Personal Data. The Company may require the individual to provide the email address the Company has on file for the individual (and verify that the individual can access that email account) as well as an address, phone number, or other data the Company has on file, to verify the individual's identity. If an agent is submitting the request on an individual's behalf, the Company reserves the right to validate the agent's authority to act on the individual's behalf.