CALIFORNIA PRIVACY NOTICE TO EMPLOYEES

Exel Inc. and Genesis Logistics Inc. (collectively, the "**Company**" or "**we**") provide this California Privacy Notice ("**Notice**") to describe our privacy practices with respect to our collection of Personal Information as required under the California Consumer Privacy Act of 2018 ("**CCPA**"). This Notice applies only to employees who reside in the State of California ("**Consumers**") and from whom we collect "**Personal Information**" as described in the CCPA. We provide you this Notice because under the CCPA, California residents who are employees qualify as Consumers. For purposes of this Notice, when we refer to Consumers, we mean you only to the extent you are an employee of the Company who resides in California.

Information we collect about Consumers.

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, on our website, your mobile device, through email, in physical locations, through written applications, through the mail, and/or over the telephone. Generally, we may collect, receive, maintain, and use the following categories of Personal Information, depending on the particular Business Purpose and to the extent permitted under applicable law:

CATEGORY	EXAMPLES
Personal Identifiers & Contact Information	Name, alias, postal or mailing address, email address, telephone number, Social Security Number, driver's license or state identification card number, passport number, employee ID number, username and password for Company accounts and systems
Physical Characteristics or Description	Eye color, hair color, hair style, height, weight, built, tattoos
Family Information	Contact information for family members listed as emergency contacts, contact information for dependents and other dependent information, medical and health information for family members related to COVID-19 symptoms, exposure, or testing, and family travel information
Information of Friends, Co-workers, and Other Associates with Whom You Have Been in Close Contact within the Past 14 Days	Medical and health information for friends, co-workers, and other associates related to COVID-19 symptoms and their travel information
Financial Information	Bank account number for direct deposit, or other financial account information

Protected Classifications	Race, ethnicity, national origin, sex, gender, gender identity, , age, disability, military status, familial status
Pre-Hire Information	Job application, resume, background check results, drug test results, job interview notes, and candidate evaluation records and assessments, work samples, voluntary disclosures
Professional or Employment-Related Information	Personnel file, 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, disciplinary records, investigatory records, training records, travel records, licensing and certification records, compensation and health benefits records, ergonomic information, COBRA notifications, and payroll information and records
Medical and Health Information	Doctor's notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, and correspondence with employee and his/her medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as post-hire drug test results, body temperature, symptoms that may be consistent with COVID-19, diagnoses of COVID-19, and medical testing relating to COVID-19
Travel Information	Locations travelled to within the 14 days prior to coming to the workplace and the dates spent in those locations
Biometric Information	Fingerprints, retina scans, facial recognition, handprint
Education Information	Information from resumes regarding educational history; transcripts or records of degrees and vocational certifications obtained
Visual, Audio or Video Recordings in the Workplace	Surveillance cameras or pictures of employees taken in the workplace or at a Company function or event, or pictures or video of employees representing the Company posted on social media
Facility & Systems Access Records	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
Geolocation Data	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

Internet, Network, and Computer Activity	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
Mobile Device Security Information	Data identifying employee devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider

How We Use Personal Information.

The Personal information we collect and our use of Personal Information may vary depending on the circumstances. This Notice is intended to provide an overall description of our collection and use of Personal Information. Generally, we may use or disclose Personal Information we collect from you or about you for one or more of the following 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 become an employee, we will use that Personal Information in connection with your employment.
2. To comply with local, state, and federal law and regulations 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), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
3. To manage and process payroll and/or Company travel and expenses;
4. To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
5. To manage workers' compensation claims.
6. To administer and maintain group health insurance benefits, 401K and/or retirement plans.
7. To manage employee performance of their job duties and/or employee conduct.
8. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
9. To evaluate job applicants and candidates for employment or promotions.
10. To obtain and verify background checks on job applicants and employees.
11. To evaluate, make, and communicate decisions regarding an employee's employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline;
12. To communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
13. To grant employees access to secure Company facilities and maintain information on who accessed the facility.
14. To implement, monitor, and manage electronic security measures on employee devices that are used to access Company networks and systems.

15. To engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
16. To communicate with employee's family or other contacts in case of emergency or other necessary circumstance.
17. To manage employee recognition programs.
18. To promote and foster diversity and inclusion in the workplace.
19. To identify potential symptoms linked to COVID-19 (including through temperature checks, antibody testing, or COVID-19 questionnaire), protect employees and customers from exposure to COVID-19, permit contact tracing relating to any potential exposure, communicate with employees and customers regarding potential exposure to COVID-19, and reduce the risk of spreading the disease in or through the workplace.
20. To provide services to corporate customers who may request certain pieces of information about a Company employee (such as name, phone number, and headshot) in order 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.

Contacting us about this notice.

If you have any questions or concerns regarding our use of Personal Information as described in this Notice, please contact the Corporate Data Protection team at Privacy.Policy@DPDHL.com .