ODW LOGISTICS, INC.

NOTICE AT COLLECTION FOR CALIFORNIA EMPLOYEES AND APPLICANTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA) AND THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020 (CPRA)

ODW Logistics, Inc. collects and uses personal information of our employees and job applicants, including sensitive personal information, for human resources, employment, benefits administration, health and safety, and business-related purposes and to be in legal compliance/the business purposes listed in the chart below. We are committed to properly handling the personal information collected or processed in connection with your employment relationship with us.

We do not sell the personal information collected for these purposes. Nor do we share it with third-parties for cross-context behavioral advertising.

Our full privacy can be found at www.odwlogistics.com/privacy/California.

We may collect the personal information and sensitive personal information categories listed in the table below. The table also lists, for each category, our expected retention period, and collection and use purposes.

Personal Information Category	**Retention Period** (from date of employment termination)	**Purpose for Collection and Use**
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.	Employee Retirement Benefit Plan information, ERISA – 6 years Federal/State withholding and disclosure – 4 years Payroll/ Timekeeping – 3 years Insurance companies – 3 years	• 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 complying with record retention requirements • Provide employees with human resources management services and employee data maintenance and support services

	Background and drug screen – 1 year Some D.O.T. exceptions – 5 years	• 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 the Company property, including information systems, electronic devices, network, and data • Ensure employee productivity and adherence to Company policies • Conduct internal audits and investigate complaints, grievances, and suspected violations of Firm policy • Respond to law enforcement requests and as required by applicable law or court order • Exercise or defend the legal rights of the Company and its employees,/ and affiliates, customers contractors, and agents
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,	1 year – 3 years Some Dep't. of Transportation drug screens – 5 years	• Comply with federal and state equal employment opportunity laws • Design, implement, and promote the Company's diversity and inclusion programs • Perform workforce analytics, data analytics, and benchmarking • Conduct internal audits, grievances, and suspected violations of Company policy • Exercise or defend the legal rights of the Company and its employees and affiliates, customers, contractors, and agents.

gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, reproductive health decisionmaking, military and veteran status.		
Internet or other similar network activity information, including all activity on the Company's 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 company-issued devices).	90 days	• Facilitate the efficient and secure use of Company information systems • Ensure compliance with Company information systems policies and procedures. • Comply with applicable state and federal laws • Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information • Enhance employee productivity • Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy • Exercise or defend the legal rights of the Company and its employees and affiliates, customers, contractors, and agents.
Geolocation data, such as the time and physical location	1 year	• Improve safety of employees, customers, and the public regarding use

related to use of an internet website, application, or device, and GPS location data from mobile devices of employees who participate in various employee benefits programs or who operate Company vehicles.		of the Company property and equipment • Prevent unauthorized access, use, or loss of the Company property • Improve efficiency, logistics, and supply chain management • Ensure employee productivity and adherence to the Company's policies • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company's policy
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, union membership, professional	1 year – 3 years ERISA – retirement benefits – 6 years	• 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 the Company's property, including its information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to the Company policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy.

affiliations, health data concerning employee and their family members.		• Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development • Exercise or defend the legal rights of the Company and its employees, and affiliates, customers, contractors, and agents
Non-public education information, such as education records, degrees and vocational certifications obtained, report cards, and transcripts.	1 year	• Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company.
Bank account information	1 year	• Direct deposit for pay and compensation

Sensitive personal information is a subtype of personal information consisting of specific information categories. While we collect information that falls within the sensitive personal information categories listed in the table below, we do not collect or use sensitive personal information to infer characteristics about a person.

Sensitive Personal Information Category	**Retention Period** (from date of employment termination)	**Purpose for Collection and Use**
Social security, driver's license, state identification card, or passport number	Employee Retirement Benefit Plan information, ERISA – 6 years Federal/State withholding and disclosure – 4 years Payroll/	**Recruitment, Onboarding, and Employment Verification**. For example, processing employment applications by verifying candidates' eligibility and conducting background checks to ensure they meet the company's hiring criteria. **Human Resources Management and Employee Services.** For example, managing payroll, administering employee benefits, maintaining personnel records, and

	Timekeeping – 3 years Insurance companies – 3 years Background and drug screen – 1 year Some D.O.T. exceptions – 5 years	communicating with employees and their beneficiaries regarding HR-related matters. **Legal Compliance and Policy Enforcement.** For example, ensuring compliance with labor laws, conducting internal audits, investigating policy violations, and responding to legal requests regarding employment practices and workplace policies. **Security and Productivity Monitoring.** For example, implementing measures to prevent unauthorized access to company assets, including information systems and data, while monitoring employee productivity and adherence to company policies
Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	1 year	Direct deposit for pay and compensation
Precise geolocation	1 year	**Safety Improvement and Asset Protection.** For example, implementing safety measures and protocols to enhance the safety of employees, customers, and the public when using company property and equipment while preventing unauthorized access and use. **Operational Efficiency and Compliance.** For example, optimizing logistics and supply chain processes to improve operational efficiency, while ensuring employee productivity and conducting internal audits to maintain compliance with company policies.
Racial or ethnic origin, religious or	1 year – 3 years	**Compliance and Legal Rights Protection.** For example, ensuring adherence to federal and state equal employment opportunity laws,

philosophical beliefs, or union membership.		and taking legal actions to protect the rights and interests of the company, its employees, and affiliates. **Diversity, Inclusion, and Workforce Analytics.** For example, designing programs that promote diversity and inclusion within the company, and utilizing data analytics for workforce assessments and insights. **Internal Governance and Policy Enforcement.** For example, conducting internal audits, investigating grievances, and enforcing company policies to ensure compliance and maintain organizational integrity.

We may contract with workforce management service providers to collect personal information on our behalf, including Ultimate Kronos Group.

If you have any questions about this Notice or need to access this Notice in an alternative format due to having a disability, please contact info@odwlogistics.com and 614-681-8523.

Effective Date: June 29, 2023