

## BIOMETRIC DATA PRIVACY POLICY

Ruan Transportation Management Systems, Inc. and its subsidiaries (together, the “Company”) uses a DriveCam® camera, or similar technology, in most of its vehicles as part of its Video Safety Program (the “VSP”) to assess and coach employees for the purpose of, among other things, enhancing road safety. The DriveCam® technology takes video of employees and may collect, capture, store, retain, and/or use Biometric Data, as defined below. This policy applies to routine operators of a truck, technicians, or other Company employees who may occasionally operate a truck or other Company vehicle (the “Driver”).

The purpose of this Biometric Data Privacy Policy (“Policy”) is to define the procedures for the collection, capture, use, safeguarding, storage, retention, disclosure, and destruction of Biometric Data. The Company’s Policy is to protect, use, store, and delete Biometric Data in accordance with all applicable laws.

**1. Biometric Data Defined.** “Biometric Data,” as used herein, refers to voiceprints, scans or imagery of the retina, iris, fingerprints, palm, vein patterns, hand or face geometry, and all other forms of data generated from the measurement or technological processing of an individual’s physiological, biological, or behavioral characteristics and that identify an individual, whether individually or in combination with other data, including, without limitation, (a) “biometric information” as that term is defined in the Illinois Biometric Information Privacy Act, 740 ILCS 14/10 (“BIPA”); (b) “biometric identifier” as that term is collectively defined in BIPA, the Texas Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code Ann. § 503.001(a), Wash. Rev. Code § 19.375.010(1), the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303(2.5) (eff. 7/1/2025) and the California Consumer Privacy Collection Act, Cal. Civ. Code § 1798.140(c); and (c) “biometric data” as that term is defined in the Washington My Health My Data Act, Wash. Rev. Code § 19.373.010(4) and Colo. Rev. Stat. § 6-1-1303(2.4) (eff. 7/1/2025).

**2. Purpose for Collection of Biometric Data.** The Company, its vendors, and/or Lytx, Inc. (“Licensor”) collect, capture, store, use, retain, and share amongst them, the Biometric Data solely for the purposes of the VSP. The Company may pay its vendors and Licensor for products or services used by the Company that utilize such Biometric Data and Licensor may use the Biometric Data for product improvement and development. The Company, its vendors, and/or the Licensor will not otherwise sell, lease, trade, or otherwise profit from any Driver’s Biometric Data.

**3. Authorization.** To the extent the Company, its vendors, or Licensor collects, captures, purchases, receives through trade, or otherwise obtains Biometric Data relating to any Driver, the Company once notified, shall as reasonably promptly as possible:

- 3.1** Inform the Driver (or his/her legal representative) in writing that Biometric Data is being collected, captured, stored, used, or retained and that the Company is providing such Biometric Data to its vendors and Licensor;
- 3.2** Inform the Driver (or his/her legal representative) in writing of the specific purpose and length of time for which any Biometric Data is being collected, captured, stored, and used; and,
- 3.3** Receive a written release signed by the Driver (or his/her legal representative) authorizing the Company, its vendors, and/or the Licensor to collect, capture, use, retain, purchase, receive through trade, or otherwise obtain Biometric Data for the specific purpose disclosed by the Company, and for the Company to provide such Biometric Data to its vendors and Licensor.

The Driver (or his/her legal representative) may revoke such release in accordance with the Company’s Biometric Data Consent and Release. Such release, however, may be a condition of employment and, thus, the Driver may be terminated from his/her employment with the Company if he/she refuses or revokes such consent for the Company to collect Biometric Data.

**4. Biometric Data Storage.** The Company shall use a reasonable standard of care to store, transmit, and protect from disclosure all Biometric Data collected or possessed by the Company. The storage,

transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits, and protects other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as: genetic markers, genetic testing information, unique identifier numbers to locate accounts or property, account numbers, PIN numbers, pass codes, driver's license numbers, or social security numbers. The storage, transmission and protection from disclosure of Biometric Data shall be in a manner that meets the standard of care in the industry.

**5. Retention Schedule.** The Company shall permanently destroy a Driver's Biometric Data, and shall request that its vendors and Licensor permanently destroy such data, when the first of the following occurs:

- 5.1** when the initial purpose for collecting or obtaining the Biometric Data has been satisfied, such as the Driver is no longer employed by the Company, or within 45 days after the Company determines storage of the Biometric Data is no longer necessary, adequate or relevant to such purpose;
- 5.2** when the Driver (or his/her legal representative) revokes his/her consent to the Company for it, its vendors, or its Licensor to collect, capture, use, retain, purchase, receive through trade, or otherwise obtain Biometric Data, as described herein; or
- 5.3** within two (2) years of the Driver's last interaction with the Company;

unless the Company is required by a statute, rule, or other law to continue to retain such Biometric Data. The Company shall at least annually conduct a review of whether the continued storage of a Driver's Biometric Data is necessary, adequate or relevant to the VSP.

**6. Disclosure.** As part of this Policy, the Company will not disclose, redisclose, or otherwise disseminate a Driver's Biometric Data, other than its vendors and the Licensor providing products or services using the Biometric Data unless:

- 6.1** The Company obtains the Driver's (or his/her legal representative's) prior consent to disclosure, redisclosure, or dissemination of the Driver's Biometric Data;
- 6.2** The disclosed Biometric Data completes a financial transaction request or authorized by the Driver(or his/her legal representative) whose Biometric Data is disclosed;
- 6.3** Disclosure is required by state or federal law or municipal ordinance; or
- 6.4** Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(rev February 5, 2025)