

Global Privacy Notice

C.H. Robinson – Biometric Data Policy

Purpose: C.H. Robinson Worldwide, Inc., and its subsidiaries (collectively, Company") has adopted this Biometric Data Policy and Notice (this "Policy") to provide guidelines for how it, its vendors, and/or the licensor of C.H. Robinson collect, store, or use Biometric Data solely for driver identification verification purposes. Protecting the confidentiality and integrity of Biometric Data is a critical responsibility that must be taken seriously at all times. Compliance with this Policy is mandatory.

Scope: Applicable to individuals residing in states with comprehensive biometric data privacy laws, including but not limited to Illinois and California, providing biometric data as defined in this policy.

Definitions: As used in this policy, "Biometric Data" includes "Biometric Identifiers" and "Biometric Information" as defined in the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, et seq., and inclusive of "Biometric Information" defined in the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act ("CPRA") Section 1798.140(c).

"Biometric Identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric Identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric Identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric Identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric Identifiers do not include information captured from a patient in a healthcare setting or information collected, used, or stored for healthcare treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act ("HIPAA") of 1996. Biometric Identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric Information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's Biometric Identifier used to identify an individual. Biometric Information does not include information derived from items or procedures excluded under the definition of Biometric Identifiers.

"Written Release" means informed consent, in written or electronic signature (an electronic sound, symbol, or process attached to or logically associated with a record).

Authorization: To the extent that the Company, its vendors, and/or the licensor of the Company's identity verification software collect, capture, or otherwise obtain Biometric Data relating to a driver, the Company will first:

- a. Inform the driver in writing that the Company, its vendors, and/or the licensor of the Company's identity verification software are collecting, capturing, or otherwise obtaining the driver's

Global Privacy Notice

C.H. Robinson – Biometric Data Policy

Biometric Data and that the Company is providing such Biometric Data to its vendors and the licensor of Company's identification verification software;

- b. Inform the driver in writing of the specific purpose and length of time for which the driver's Biometric Data is being collected, stored, and used; and
- c. Receive a written release signed by the driver (or his or her legally authorized representative) authorizing the Company or its vendor(s) of Company's identification verification software to collect, store, and use the driver's Biometric Data for the specific purposes disclosed by Company, and for Company to provide such Biometric Data to its vendors and the licensor of Company's identification verification software.

The Company, its vendors, and/or the licensor of the Company's identification verification software will not sell, lease, trade, or otherwise profit from drivers' Biometric Data; provided, however, that the Company's vendors and the licensor of the Company's identification verification software may be paid for products or services used by the Company that utilize such Biometric Data.

Disclosure: The Company will not disclose or disseminate any Biometric Data to anyone other than its vendor(s) of the Company's identification verification software without/unless:

- a. Obtaining written driver consent to such disclosure or dissemination;
- b. The disclosed Biometric Data completes a financial transaction requested or authorized by the driver;
- c. Disclosure is required by state or federal law or municipal ordinance; or
- d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention and Destruction Schedule: The Company will have access to Biometric Data for 60 days after it is provided, however Company will not store such Biometric Data on its servers. Rather the Biometric Data will be stored on the servers of the licensor of the Company's identification verification software. Any driver's Biometric Data in the Company's possession will be retained only until the first of the following occurs:

- a. The initial purpose for collecting or obtaining such Biometric Data has been satisfied, such as the termination of the driver's employment, or the driver moves to a role for which the Biometric Data is not used; or,
- b. Within 3 years of the driver's last interaction with the identification verification software.

Privacy Protection: The Company will use a reasonable standard of care to store, transmit, and protect any paper or electronic Biometric Data collected from disclosure. Such storage, if any, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than

Global Privacy Notice

C.H. Robinson – Biometric Data Policy



how the Company stores, transmits, and protects from the disclosure of other confidential and sensitive information outlined in its [Privacy Notice](#).