Biometric Data Collection and Retention Policy

Ascend, LLC and its affiliated entities (collectively referred to as "Ascend") may collect, store, and use Biometric Data for certain purposes described below, and it may disclose that Biometric Data in certain circumstances. This Policy explains what that means for you, and how you consent to Ascend's activities.

Definitions

"Biometric Data" as used in this Policy includes both: (i) "Biometric Identifiers", meaning a facial, retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry or other physiological traits. Biometric Identifiers do not include writing samples, written signatures, photographs, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color; and (ii) "Biometric Information", meaning any information, regardless of how it is captured, converted, stored, or shared, that is based on Biometric Identifiers, including a facial, retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, that is used to identify an individual.

Data Collection and Purpose

Ascend uses AI dash cameras and software technology to manage our fleet and improve driver safety. AI Dash Camera vendors used by Ascend include, but are not limited to, Samsara, Omnitracs Smart Drive, Trimble Peoplenet or Netradyne (each a "Vendor"). Vendor AI Dash Cams includes both a road-facing camera to capture video footage of critical events, along with an inward facing camera. The inward facing camera includes a feature called Camera ID, which relies on facial and voice recognition technology to identify drivers. The facial recognition technology operates, in part, through scans of a driver's face geometry and use of voiceprints. Both of these items are considered Biometric Data under Illinois law. Vendor's technology allows Ascend to use this Biometric Data to assign drivers to vehicles, assign trips, and to analyze harsh driving events in the Vendor Dashboard. Using the features on Vendor's camera enhances safety by increasing the efficacy of Vendor's driver-based insights and also helps Ascend maintain accurate logs of our operations.

The Biometric Data collected using Vendor's Camera ID will be disclosed to Vendor and stored on Vendor's Cloud Dashboard. Vendor will have access to the Biometric Data to perform the functions of its services agreement with Ascend. A copy of Vendor's privacy policy is available at

- Samsara: https://www.samsara.com/support/privacy/
- Netradyne: https://www.netradyne.com/privacy-policy
- Omnitracs Smart Drive: https://www.omnitracs.com/privacy-policy
- Trimble Peoplenet: https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center?tab=privacy_notice

Data Storage, Protection and Disclosure Policy

Ascend's policy is to protect and store Biometric Data in accordance with applicable laws and regulations, including, but not limited to, the Illinois Biometric Information Privacy Act. Specifically, Ascend shall use a reasonable standard of care to store, transmit and protect from disclosure any Biometric Data collected. Such 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 Ascend stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual such as social security numbers.

Biometric Data collected from drivers using Vendor's AI dash cameras will not be disclosed to parties other than Ascend or Vendor, except in the following circumstances: (1) after Ascend obtains appropriate written consent from the driver(s); (2) when disclosure completes a financial transaction requested or authorized by the driver(s); (3) when disclosure is required by federal, state, or local law; or (4) when disclosure is required by a valid subpoena or warrant issued by a court. Within Ascend, the Biometric Data may be shared with only those employees who have a need to know for a specific business purpose.

Retention and Destruction of Biometric Data

Ascend will retain the Biometric Data during the time that an individual is employed or engaged by Ascend in a role for which the Vendor AI Dash Cam is used. Within a reasonable time after the conclusion of the employment or contractor relationship, or upon an employee's transfer to a position for which the Vendor AI Dash Cam is not utilized, whichever occurs first, Ascend will permanently delete the Biometric Data that it retained, except in the following circumstances: (1) after Ascend obtains appropriate written consent from the driver(s); (2) when retention is required by federal, state, or local law; (3) when retention is required by a valid evidence preservation letter, subpoena or warrant issued by a court or (4) when the retention is necessary to preserve evidence related to a motor vehicle accident or in Ascend's reasonable anticipation of litigation resulting therefrom.

Consent Form

Before you begin or continue employment or engagement with Ascend in a role for which the Vendor AI Dash Cam is used, you must execute the *Notice and Consent to Collection of Biometric Data* form accompanying this Policy.