Biometric Privacy Policy

This Policy applies to all ZKTeco USA (the "Company") employees, agents, contractors, customers, or third parties engaged with the Company who have authorized access to Biometric data (templates) the Company has collected or otherwise has in its possession.

Explanation how Biometric Technology works:
The enclosed device uses biometric technology to recognize & record individuals interacting with the device. When an individual enrolls or authenticates themselves to the device, the device temporarily captures & stores an image of that individual's biometric identifier (i.e., fingerprint, face, finger-vein, palm-vein, iris, etc.), but only for so long as needed to create that individual's biometric data (template) used for subsequently recognizing & recording that same individual. Thereafter, only the biometric template is stored, which is a binary computer file (not an image) representing a tiny subset of that individual's biometric identifier. After an individual's biometric template is generated, the individual's biometric identifier (acquired image) is immediately and permanently deleted from the device.

Fingerprint/face/palm images are NOT stored by default
Aside from the temporary storage of an individual's biometric identifier, the device does not permanently store an individual's biometric identifier, nor create or store images thereof, absent an independent affirmative decision and action on the part of the individual or customer to do so.

Biometric templates are stored in BOTH the device and Company cloud
Customer's biometric templates are stored in both the device and optionally, the Company's cloud. Company uses a reasonable standard of care to guard against unauthorized access to and acquisition of the biometric templates, which will be reasonable for the Company's industry, in a manner that is the same or exceeds the standards used to protect other confidential information held by the Company.

Customer is solely responsible for deleting Biometric templates
The Company will NOT destroy any biometric templates, regardless the status of an individual associated with the customer. ONLY the customer can destroy biometric templates of individuals associated with the customer. Therefore, the Company strongly advises the customer to destroy biometric data when the initial purpose for obtaining or collecting such biometric data has been fulfilled or within six months of the associated individual's last interaction with the customer, whichever occurs first.

#

Be advised that certain states in the U.S. have enacted privacy laws governing the collection and storage of an individual's biometric data.

The customer who purchases the enclosed device and uses it to collect and/or store biometric data is solely responsible for ensuring the customer's compliance with applicable biometric privacy laws in any applicable state.

The Company is not responsible and shall not be held liable for use of this device by customers in a manner that is not compliant with the Company's biometric privacy policy and applicable privacy laws.

Advisable to gain employees' consent prior to collecting their biometric data
The Company strongly encourages customers purchasing this device to provide adequate notice and obtain prior written consent from the individuals who will be interacting with the device before collecting and storing the individuals' biometric templates.

The Company further encourages customers of this device to consult with legal counsel knowledgeable in the area of biometric privacy, especially if the customer operates in state(s) which have enacted privacy laws governing the collection and/or storage of an individual's biometric data.

The customer is solely responsible for taking any steps necessary to ensure that the customer is in compliance with applicable biometric privacy laws when using this device. Nothing in this notice is intended to constitute or provide legal advice to any customer.

#