BIOMETRIC PRIVACY NOTICE

5/1/2020

This device uses biometric technology to recognize and register individuals who interact with the device.

Please note that biometric data is considered as personal identification information and as such should be considered as specially protected accordingly.

When a person enrolls or authenticates into the device, the device captures and temporarily stores an image of that person's biometric identifier (i.e. fingerprints, face, finger veins, palm veins, iris, etc.), but only for the time required to create the biometric template for that person, which is used to subsequently recognize and enroll that same person. The resulting permanently stored biometric template is only a binary computer file (not an image) representing a tiny subset of that individual's biometric identifier. Once an individual's biometric template is generated, the individual's biometric identifier (acquired image) is immediately and permanently deleted from the device.

THE ONLY EXCEPTION IS ZKTECO BIOMETRIC DEVICES CAPABLE OF DETECTING BODY TEMPERATURE (BTD).

CUSTOMERS HAVE THE OPTION TO ACTIVATE THE FUNCTION "CAPTURE ALL FACE PHOTOS OF REGISTERED AND UNREGISTERED USERS". WHEN THIS FEATURE IS ACTIVATED, ALL PHOTOS OF THE USERS' FACE WILL BE CAPTURED AND STORED IN THE DATABASE OF ZKTECO SOFTWARE. CUSTOMERS CAN DECIDE WHERE TO INSTALL THE DATABASE. IT IS IMPORTANT TO NOTE THAT ZKTECO DOES NOT HAVE ACCESS TO THE CLIENT DATABASE. ONLY THE CLIENT HAS ACCESS TO THE DATABASE.

Aside from enabling the "CAPTURE ALL PICTURES OF REGISTERED AND UNREGISTERED USERS" function on BTD devices, ZKTeco devices do not normally permanently store an individual's biometric identifier, nor do they create or store images of the individual, in the absence of an independent decision and affirmative action by the individual or client to do so.

The customer who purchases the attached 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 state.

Please note that ZKTeco is simply the manufacturer of this device.

ZKTeco does not collect, store, or access data collected and stored by the customer who purchases this device.

ZKTeco and its affiliates are not responsible or liable for customers' use of this device in a manner that does not comply with applicable privacy laws.

Accordingly, ZKTeco strongly recommends that customers who purchase this device properly notify the data subject and have a legal basis for the processing, such notification must be

prior to and directed to the individuals who will be interacting with the device and prior to collecting and storing the data from such individuals.

In addition, ZKTeco recommends that customers of this device consult legal counsel with expertise in the field of biometric data protection, especially if the customer operates in one or more states that have enacted data protection laws regulating the collection and/or storage of a person's biometric data. In this regard, the General Data Protection Regulations require that the data controller carry out an Impact Assessment to make use of the biometric data of employees to determine the proportionality of these biometric identification systems. The controller will also consult the supervisory authority before proceeding with the processing where a data protection impact assessment under Article 35 GDPR shows that the processing would involve a high risk if the controller does not take measures to mitigate that risk.

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

1600 Union Hill Rd.
Alpharetta, GA 30005
862 505 1201
www.zktecousa.com

GUIDELINES ON THE USE OF BIOMETRIC DATA

Biometric Data User refers to any person who collects or use biometric data utilizing ZKTeco's device, hardware

and software

1. The purpose of biometric data collection

1.1. Use of biometric data & related activities

It is data user's responsibility to inform all users or persons whose biometric data are collected, that all the collected biometric data are only used for time attendance and access control purposes.

1.2. Lawful and fair means Data User must collect users' biometric templates only on a legal and fair basis.

1.3. Adequate but not excessive

ZKTeco's devices and all biometric templates stored in its management software are built with precise algorithms, and may be in various methods encrypted, in order to prevent data leakage of users to the greatest extent.

2. Accuracy and Duration of Retention

2.1. Accuracy of personal data held

ZKTeco, with rich experience of software and hardware development, to the greatest extent ensures that all biometric data and personal data are stored accurately, in order to provide customers best user experience.

2.2. Personal data not being kept longer than is necessary

When using ZKTeco's software and hardware, data user is responsible for ensuring that all users' data are not stored in ZKTeco's software and hardware unless necessary.

2.3. Prevent any personal data transferred to the data processor from being kept longer than necessary

ZKTeco's hardware applies different biometric templates during operation, but all templates are not remained in the CPU of the hardware, and after users' biometric templates are

deleted in ZKTeco's hardware and software (according to actual situation), the templates are permanently deleted and not remained in any format.

3. Use of Personal Data

3.1. Not being used for a new purpose without prescribed consent If data user wishes to apply the collected biometric templates to any purpose other than any use authorized, they are responsible for reintroducing to the users and obtain their consents before doing so.

4. Security of Personal Data

4.1. Practicable steps being taken to ensure no unauthorized or accidental access, processing, erasure, loss, use and transfer. ZKTeco's applied biometric algorithms do not collect complete biometric features of the collected persons, instead only 10 to 50 feature points are collected for calculation. Even if biometric templates are illegally obtained, it is not possible to reorganize them into complete biometric features. In ZKTeco's software and hardware, various advanced electronic encryption techniques have been applied for the greatest extent of protection to data security.

5. Openness – Information be Generally Available

5.1. Data User should provide policies and practices in relation to personal data.

5.2. Data User should publicize the kinds of biometric data held.

5.3. Data User should inform the main purposes for which biometric data are used.

6. Access to Personal Data

6.1. Data user should know that, all data subjects have the rights to access and correct his or her personal data.

Frequently ask question of biometric data:

I. What is Biometric Data?

Physiological data born with an individual

– DNA samples, fingerprint, palm veins, iris, retina

– Facial images and hand geometries

– Behavioral data developed by an individual

– hand writing pattern, typing rhythm, gait, voice

II. Is Biometric Data Personal Data?

Biometric data alone is not regarded as personal data according to law, as it may not reveal identities. However, if biometric data is stored in a database that links customers/staff members, they are personal data.

III. Is Biometric Template Personal Data?

If biometric data is not stored, but only is displayed as representation (called a template), and is encrypted and stored as a meaningless number, then it is not personal data. But if an organization can decrypt the number and links it to an individual, it is personal data

1600 Union Hill Rd.
Alpharetta, GA 30005
862 505 1201
www.zktecousa.com

HIPPA guidelines are designed to protect the health records of patients. Conversely, SpeedFace+ is designed to detect and report upon employees' and visitors' (not patients') detected body temperature. Also note that SpeedFace+ recorded data is stored inside the customer's network. ZKTECO has NO ACCESS to SpeedFace+ recorded data. Therefore, SpeedFace+ recorded data should be managed by the customer, no differently than the customer currently manages their existing data.

HIPAA COMPLIANCE is based on how customers UTILIZE SpeedFace+, and not the device, itself. If customers refrain from having SpeedFace+ record PATIENT body temperature and keep SpeedFace+ recorded data safe inside the customer's network, customers will typically remain HIPAA compliant while operating SpeedFace+.

FAQs For Customers Using SpeedFace+

These FAQS are intended to discuss some basic features of SpeedFace+ and provide general information for customers about data privacy and security compliance and best practices. They are not intended to completely outline a customer's obligations when implementing SpeedFace+. We do not provide legal, financial, or other advice and we recommend you consult qualified and experienced counsel for questions related to any legal, regulatory compliance, or contractual or other obligations you may have in connection with SpeedFace+ implementation.

1. What does SpeedFace+ do? SpeedFace+ is a biometric screening and security solution to assist organizations with admitting persons into their facilities. For example, SpeedFace+ records certain information of users when they attempt to enter your facilities. In the case of registered end users, the device records badge#, name, date/time stamp, and body temperature when the end user "checks in/out." In the case of unregistered end users (e.g., strangers, visitors), the device can record the body temperature and the date/time the user interacted with the device. For more information, please click here for SpeedFace++ product details.

2. What data does SpeedFace+ collect when an end user is screened? The data SpeedFace+ collects depends on whether the end user is registered. If the end user is registered, SpeedFace+ will collect and store the device number, date, time, user ID, username, and the end user's body temperature. If the end user is unregistered, SpeedFace+ will collect and store a "time stamp" that consists only of the unidentified individual's body temperature. In either case, customers can configure the device if they choose to take a picture of the end user and store that face image on the device. The device will convert the image to a biometric template and use that template going forward to verify the user.

3. Is the data collected from end users by SpeedFace+ subject to the Health Insurance Portability and Accountability Act (HIPAA)? In general, HIPAA applies to covered entities (e.g., healthcare providers and health plans) and their business associates, not employers. Accordingly, when customers use SpeedFace+ in their workplace in their role as employers, the data typically would not be subject to HIPAA. However, when HIPAA covered entities or business associates, such as health care providers, use SpeedFace+ in a health care setting to screen patients, only then the data may be subject to HIPAA. We recommend you consult with counsel to identify any potential compliance obligations. In either event, data collected using SpeedFace+ may be considered personal information and should be safeguarded.

4. We are using SpeedFace+ in our capacity as a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), what compliance steps should we thinking about?

When SpeedFace+ is used to scan and record patients only, the data collected concerning those patients likely will be considered protected health information (PHI). For covered entities, a key concern is compliance with the HIPAA Security Rule, which generally requires administrative, physical, and technical safeguards to protect the confidentiality and security of PHI. Regarding SpeedFace+, HIPAA covered entities first should conduct a documented risk assessment concerning its integration into its environment. That assessment will help the covered entity determine the threats and vulnerabilities to the data as collected and stored on the device, as well as on the covered entities information systems. Examples of safeguards to consider include password protection, encryption of data at rest, and access management. As noted above, these FAQs are not intended to completely outline your legal or compliance obligations when implementing SpeedFace+. We do not provide legal or other

advice and we recommend you consult qualified and experienced counsel for questions related to any legal and regulatory compliance.

5. Is the data collected from end users through SpeedFace+ subject to the Americans with Disabilities Act (ADA)? For customers subject to the ADA, the medical information SpeedFace+ collects from the customer's employees likely would be considered confidential medical information subject to the ADA. Those customers should implement appropriate measures to ensure the confidentiality of this data including limiting access and disclosure and maintaining reasonable safeguards. This would also require performing the screening in a manner that protects the confidentiality of the results. Since the CDC and state and local authorities have acknowledged the community spread of COVID-19, according to the Equal Employment Opportunity Commission's guidance, employers may measure employees' body temperatures based on the notion that employees present a "direct threat." However, it is possible this practice may not be permitted once the pandemic has subsided, and the EEOC no longer considers the pandemic a direct threat. Customers need to monitor these developments closely with counsel to ensure continued use of certain features of SpeedFace+ are permissible.

6. Does SpeedFace+ collect biometric information? Over the past several years, federal and state law has started to increasingly regulate the collection and safeguarding of biometric information. In Illinois, the Biometric Information Privacy Act (BIPA) contains detailed requirements for businesses seeking to collect biometric information or biometric identifiers from Illinois residents. These requirements include, among other things, notice, consent, and data destruction policies. Answering this question, therefore, depends on the specific information being considered and the law that applies.

The results of a temperature scan alone, for example, generally does not fall within the definition of biometric information or a biometric identifier under the BIPA, however, it may constitute biometric information as defined under the California Consumer Privacy Act. SpeedFace+ collects a small sub-set of sample data (aka minutia points) from the face, palm, or fingerprint. For example, SpeedFace+ includes a feature that allows customers to store a digital representation of a face image to verify the end user's identity. That is, it converts certain face image data into binary data using mathematical algorithms to create

a biometric template. SpeedFace+ stores this digital representation and not the actual image on the customer's systems. This information may constitute biometric information under BIPA and other federal or state laws. Before collecting this data from employees or others, customers should review applicable compliance requirements and be sure appropriate measures are in place. Of course, customers may turn off certain SpeedFace+ features, such as facial recognition.

ZKTECO customers are solely responsible for compliance with applicable law governing their collection, access, use, processing, storage, safeguarding, and disclosure of biometric identifiers and information from end users. The same is true for personal information generally. We recommend you consult with qualified and experienced counsel to identify any potential compliance obligations before implementing SpeedFace+.

7. Are we required to obtain the end user's consent to use SpeedFace+? Maybe. State laws such as the BIPA (see discussion above) may require customers to provide notice and obtain end user consent prior the collection of the information by SpeedFace+. If the customer deploys SpeedFace+ in countries outside of the U.S., applicable data privacy laws, such as the EU General Data Protection Regulation, may require end user consent. We recommend you consult with counsel to identify any potential compliance obligations prior using the SpeedFace+ to collect personal information.

8. Are we required to give the end user a privacy notice? Certain state laws may require the customer to provide end users with a privacy notice. For example, if the customer is subject to the California Consumer Privacy Act, it must provide a notice at collection to California residents at or before collection of personal information by SpeedFace+. For employees, this requirement remains in effect at least through 2020. If the customer deploys SpeedFace+ in Illinois, the BIPA requires that the customer provide end users in Illinois with a privacy notice regarding the collection and retention of biometric information. In addition, if the customer deploys SpeedFace+ in countries outside of the U.S., applicable data laws such as the EU General Data Protection Regulation may require end user consent. We recommend you consult with counsel to identify any potential compliance obligations.

9. How is end user data collected through SpeedFace+ stored? The SpeedFace+ software is not cloud based and the device is not connected to ZKTECO's information systems. Thus, ZKTECO neither collects, nor has access to, nor stores information including personal information from SpeedFace+. All end user data collected through SpeedFace+ is stored on the customers' systems. If the end user is registered on the device, the collected data is recorded in a log file on the device maintained by the customers. The customer has the option of transferring the log file to SpeedFace+ software running on the customer's information systems.

10. Who will have access to the end user data collected through SpeedFace+? The customer has sole control over who will have access to the end user data. ZKTECO does not have access to end user data collected by or stored in the device or in the SpeedFace+ software which runs on the customer's systems. The only time ZKTECO may be assigned temporary access to the customer end user data is if the customer initiates a trouble-shooting remote session with ZKTECO.

11. How long is the data collected from end users through SpeedFace+ retained? The customer has sole control over how long end user data is retained. Note that state and federal laws may limit the period certain information may be maintained. Customers should consult with counsel and review their record retention schedules to ensure compliance with applicable state or federal laws.

12. Does ZKTECO maintain policies concerning the collection of personal information with respect to its customers?

ZKTECO maintains several policies concerning personal information, including personal information that is collected, accessed, or stored through or on SpeedFace+ by a customer. We include a summary of those policies here.

Our customers are responsible for compliance with all applicable law and other obligations governing any collection, storage, usage, retention, destruction, breach, and/or transmission of personal information, including biometric information, they conduct or facilitate with regard to their use of SpeedFace+. That responsibility includes, without limitation, developing and implementing required notices, releases, policies and procedures, and agreements relating to such personal information.

To the extent required by law, customers should obtain written authorization from each employee or other individual necessary to collect, store, use, and/or transmit personal information.