CDVI
Security to Access

ievo

How ievo systems protect your data

Biometrics refer to distinctive, measurable human characteristics which label and describe an individual. By measuring and analysing these biological features the data can be utilised for unique security identification purposes.

INTRODUCTION

Considered to be the most reliable and trustworthy form of high class security, ievo biometric fingerprinting adds many advantages and benefits over common place security solutions. The advantage of using biometrics is that common faults like; lost, stolen or copied cards/fobs; forgotten pin numbers/or access codes; hacking threats or any other form of unnecessary user interaction are all resolved. Saving, time and resources while enhancing security access controlled systems.

ievo systems protect not only building and premises, but also individuals and increase productivity in time and attendance management.

SECURITY

Due to the nature of biometric data being unique to an individual, it opens up a lot of options for increased levels of security for identification purposes, which are more reliable, accurate and efficient than more traditional levels of security.

It is vital to understand how ievo biometric systems use and store this data, in order to give assurances to users that this information is fully protected.

Please turn over to find out more about how ievo use and store your data.

CAPTURING YOUR DATA

When registering a fingerprint an ievo system will scan and extract data using an extraction algorithm which identifies specific features within a fingerprint called minutiae.

Identified minutiae points are categorised into groups, which include line bifurcations and ridge endings amongst other data groups. After a registered scan an ievo reader will send an image of the fingerprint to the ievo control board where an advanced algorithm will identify the type, direction and distance between key minutiae features of a fingerprint (Fig.1). This data is converted into a template and stored in a database on the ievo control board. The original fingerprint image is not stored or recorded.

When using a reader for access a similar process described above will commence. However, this time the matching algorithm will be used to compare the new minutiae data against the stored templates in the database. Once a pre-set number of minutiae points have been matched against a stored template, the user's identity will be confirmed, this confirmation will be forwarded to the access control system or 'time and attendance' system for entry and/or data logging.

DATA PROTECTED

Once a fingerprint has been scanned the original image is not stored or recorded. The only recorded details are the key data points taken from a fingerprint which are transferred and stored on an ievo control board in a unique proprietary template format. The stored template is unique to an individual and the template is only accessed for identification purposes by the ievo control board. The data cannot be accessed for any other purpose nor can it be viewed using common software.

ievo systems use a cutting-edge Automated Fingerprint Identification System (AFIS) algorithm for data enrolment, extraction and matching processes. This data cannot be reverse engineered to recreate an image of the original fingerprint.

To find out more information about ievo fingerprint readers and data protection, please contact us.

YOUR DATA

An advanced extraction algorithm is used to create a template from specific fingerprint data captured after a scan. This data (Fig.2) is stored using a unique proprietary template format. All other information is not stored or recorded. The data CANNOT be used to re-construct the original fingerprint image.

SECURITY

ievo systems function with a separate control board which controls an ievo reader, meaning that no information or data is stored locally on reader units themselves. For additional security, the ievo control board, should always be installed on the secure side of an entry point, away from the reader units.

ievo readers do not house any locking mechanisms or door relays, meaning that if a reader was removed, your access point would remain secure and your data would remain safe. The reader unit would be deemed useless to the attacker, as it contains no data.

Fig.1: Image depicting what an ievo reader scans and key minutiae features.

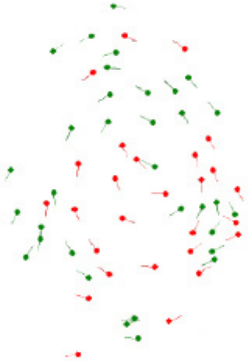

Fig.2: Image depicting key feature data which is extracted, transferred and stored as a template.

GDPR

CDVI UK Ltd does not hold or control any personal data relating to the ievo readers and will only have remote access to such personal data when providing support to end users, in which case it will be acting as a data processor and acting on the instructions of a Data Controller.

As a Data Controller, installers and end users of an ievo system must ensure that they are fully compliant with General Data Protection Regulation 2016/679 as they control the collection of data and purposes of processing in order to identify the user's fingerprint and grant access or record time & attendance.